EXHIBIT 1

AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

FILED ENTERED
LODGED RECEIVED

JUL 29 2019

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY DEPUTY

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Sixteen (16) Google accounts, hosted at premises controlled by Google LLC, located at 1600 Amphitheatre Parkway, Mountain View, CA, more fully described in Attachment A-1

Case No. MJ19-350

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Sixteen (16) Google accounts, hosted at premises controlled by Google LLC, located at 1600 Amphitheatre Parkway, Mountain View, CA, more fully described in Attachment A-1, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-1, for a list of information to be disclosed, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 371; 1029; 1030	Conspiracy; Access Device Fraud; Unauthorized Access to a Protected Computer
18 U.S.C. § 1343; 1349	Wire Fraud; Conspiracy to Commit Wire Fraud

The application is based on these facts:

✓ See Affidavit of Special Agent Andrea DeSanto continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☐ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Andrea DeSanto, Special Agent
Printed name and title

◉ The foregoing affidavit was sworn to before me and signed in my presence, or
○ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 07/29/2019

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge
Printed name and title

USAO: 2018R01422

AFFIDAVIT OF SPECIAL AGENT ANDREA L. DESANTO

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, ANDREA L. DESANTO, being duly sworn under oath, depose and say:

INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), currently assigned to the Seattle Field Office, and have been so employed since April 2006. I am assigned to the Cyber squad where I primarily investigate computer intrusions and other cybercrimes. My experience as an FBI Agent includes the investigation of cases involving the use of computers and the Internet to commit crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, cybercrimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment. I hold Bachelor of Science degrees in Mathematics and Zoology from University of Wisconsin. I hold a Masters of Business Administration from DePaul University.

2. In addition to my experience with cybercrimes investigations and prosecutions, I also have experience and training with financial investigations. I have received formal training on tracing the financial proceeds of crimes. I have applied that training in the context of dozens of investigations in which I have reviewed records from financial institutions both in the United States and in foreign jurisdictions, in order to identify the proceeds of criminal offenses under investigation. Prior to my assignment to the Cyber squad, I was assigned to the White Collar Crime squad, where my primary duties included investigating corporate fraud and identity theft.

3. Prior to my employment as a Special Agent, I worked as a software/database developer for approximately ten years. As part of that employment, I became familiar with

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

the design and operations of various electronic devices, networks, and websites, including technology described herein.

PURPOSE OF AFFIDAVIT

4. I make this affidavit in support of applications for a search warrant for information associated with the following accounts:[1]

a. The accounts registered to amazonnate11[@]gmail.com ("SUBJECT ACCOUNT 1"), joe[@]digitalcheckmate.com ("SUBJECT ACCOUNT 2"), jn[@]sellerstrategies.com ("SUBJECT ACCOUNT 3"), [redacted][@]gmail.com ("SUBJECT ACCOUNT 4"), kml[@]digitalcheckmate.com ("SUBJECT ACCOUNT 5"), [redacted][@]gmail.com ("SUBJECT ACCOUNT 6"), freakdaze[@]gmail.com ("SUBJECT ACCOUNT 7"), [redacted][@]googlemail.com ("SUBJECT ACCOUNT 8"), [redacted][@]gmail.com ("SUBJECT ACCOUNT 9"), [redacted][@]gmail.com ("SUBJECT ACCOUNT 10"), [redacted][@]gmail.com ("SUBJECT ACCOUNT 11"), [redacted]@]gmail.com ("SUBJECT ACCOUNT 12"), ellekaye11[@]gmail.com ("SUBJECT ACCOUNT 13"), rogerparkin69[@]gmail.com ("SUBJECT ACCOUNT 14"), [redacted][@]gmail.com ("SUBJECT ACCOUNT 15"), [redacted][@]gmail.com ("SUBJECT ACCOUNT 16"), which are stored at premises controlled by Google LLC ("Google"), an email provider headquartered in Mountain View, California.

b. The account [redacted][@]yahoo.com ("SUBJECT ACCOUNT 17"), which is stored at premises controlled by Oath Holdings, Inc., formerly known as Yahoo Holdings, Inc. and doing business as Yahoo! ("Yahoo"), an email provider headquartered in Sunnyvale, California.

c. The Facebook accounts bearing profile identification numbers 557853344 ("SUBJECT ACCOUNT 18"), 23004459 ("SUBJECT ACCOUNT 19"), and

---

[1] I have bracketed portions of email addresses discussed in this affidavit to ensure that they are not inadvertently hyperlinked and contacted by anyone reading an electronic copy of this document.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

607905026066065 ("SUBJECT ACCOUNT 20"), which are stored at premises controlled by Facebook, Inc., a social networking company headquartered in Menlo Park, California.

d. The Apple iCloud accounts registered under kristenleccese[@]gmail.com, bearing digital sign identifier 10075071322 ("SUBJECT ACCOUNT 21") and joe[@]digitalcheckmate.com, bearing digital sign identifier 1712170805 ("SUBJECT ACCOUNT 22"), which are stored at premises controlled by Apple, Inc., an electronic communications service and remote computing service provider headquartered in Cupertino, California.

e. The LinkedIn account bearing screenname "joenilsenseo" ("SUBJECT ACCOUNT 23"), which is stored at premises controlled by LinkedIn Corporation, an electronic communications service headquartered in Sunnyvale, California.

f. The Quora accounts registered to joe[@]digitalcheckmate.com ("SUBJECT ACCOUNT 24"), kristenleccese[@]gmail.com ("SUBJECT ACCOUNT 25"), and kml[@]digitalcheckmate.com ("SUBJECT ACCOUNT 26"), which are stored at premises controlled by Quora Inc., an electronic communications service headquartered in Mountain View, California.

g. The Dropbox cloud-storage account registered to user number [redacted][@]gmail.com, namely account number [redacted] ("SUBJECT ACCOUNT 27"), which is stored at premises controlled by Dropbox, Inc., an electronic communications service and remote computing service provider headquartered in San Francisco, California.

SUBJECT ACCOUNTS 1 through 27 are collectively referred to herein as the "SUBJECT ACCOUNTS."

5. The information to be searched is described in the following paragraphs and in Attachments A-1 through A-7. This affidavit is made in support of applications for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require the providers named above to disclose to the government copies of the information (including the content of communications) relating to the SUBJECT ACCOUNTS, as further described

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

in Section I of Attachments B-1 through B-7. Upon receipt of the information described in Section I of Attachments B-1 through B-7, government-authorized persons will review this information to locate the items described in Section II of Attachments B-1 through B-7.

6. The requested warrants authorize a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrants in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

7. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that evidence, instrumentalities, contraband, and/or fruits of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected Computer), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud), will be found in the SUBJECT ACCOUNTS. In addition, and as discussed below, there is probable cause to believe that the SUBJECT ACCOUNTS were used in furtherance of the criminal scheme under investigation.

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States (including a magistrate judge of such a court) . . . that has jurisdiction over the offense being investigated," 18 U.S.C. § 2711(3)(A)(i), and "is in . . . a district in which the provider . . . is located or in which the wire or electronic communications, records, or other information are stored." 18 U.S.C. § 2711(3)(A)(ii).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

STATEMENT OF PROBABLE CAUSE

9. In or about December 2018, Amazon.com, Inc. ("Amazon") submitted a criminal referral to the FBI regarding fraudulent activity on an online platform operated by Amazon, which is commonly referred to as "Amazon Marketplace." According to records maintained by the Secretary of State of Washington State, Amazon is a corporation that was incorporated in Delaware on or about May 28, 1996. Amazon has been authorized to do business in Washington since on or about June 18, 1996.

A. Background Regarding Amazon Marketplace

10. As Amazon's website explains, the term "Amazon Marketplace" refers to a virtual marketplace through which Amazon permits third-party sellers to market products to consumers who visit the website amazon.com. Amazon states that the benefits to sellers of marketing goods on Amazon Marketplace include:

a. The ability to "[r]each hundreds of millions of customers" by accessing "a massive audience of confident customers—in the U.S. alone, Amazon has over 150 million unique visitors. Benefit from a brand that ranks #1 in reputation as determined by a 2018 Nielsen Company survey."[2]

b. The ability to "[l]et us do the heavy lifting" because sellers can "[s]cale swiftly and reach even more customers with Fulfillment by Amazon, our world-class fulfillment service. We pick, pack, and ship your products and take care of customer service and returns—all so you can focus on growing your business."[3]

c. The ability to "[g]et your products seen by more shoppers" because sellers can "[i]ncrease your reach and drive sales by advertising your products on Amazon. Keyword-targeted ads appear in high-visibility placements, right where customers will see them, and you only pay when your ad is clicked."[4]

---

[2] *See* https://services.amazon.com/content/sell-on-amazon.htm, *last accessed on* May 28, 2019, 4:11 p.m.
[3] *Id.*
[4] *Id.*

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

11. In exchange for listing, advertising, and managing the "fulfillment" of sellers' products on Amazon Marketplace, Amazon charges sellers certain fees. These fees include a monthly subscription fee to list up to forty products (or, in the alternative, a per-product listing fee). Sellers also may be charged "referral" and "closing" fees, depending on a product's type or cost. Amazon also charges sellers fees associated with the "fulfillment" of their product orders—*i.e.*, fees to pick up, pack, ship, store, and handle customer service and refunds for product orders. As with the referral and closing fees, the costs that sellers must pay for product "fulfillment" depend on the type of product (*e.g.*, its size).[5]

12. Based on my review of Amazon's website (www.amazon.com), I learned that Amazon assigns an individual webpage to each product listing by a third party (referred to herein as a "product page"). The product page sets forth substantial information about the product, including information that the website visitor needs in the event she chooses to purchase the product and hyperlinks to other information about the product. The information on the product page includes but is not limited to the following:

a. Product Name and Description: The product page typically includes several photographs of the advertised product, along with a product name that appears in bolded font at the near the top of the webpage. The product page also sets forth the product's specifications, such as a bulleted list of product features, the product's dimensions and weight, the manufacturer-assigned model number, and the Amazon-assigned Amazon Standard Identification Number or "ASIN number." ASIN numbers are numbers that Amazon assigns to products listed on the Amazon Marketplace, which Amazon use in order to track information about products. If two sellers list the same product for sale, then both product's product pages will list the same ASIN number.

---

[5] In addition to providing third parties with a marketplace on which to sell their products, Amazon itself lists products for sale on Amazon Marketplace. Amazon's own product listings are not currently the subject of the Government's investigation and, therefore, are not addressed herein. According to Amazon's website, "more than 50% of Amazon's total unit sales come from third-party selection." *See* https://services.amazon.com/selling/benefits.htm, *last accessed on* May 29, 2018 (3:39 p.m. PST).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Purchasing Information: The product page also typically includes information that pertains to the potential purchase of the product, including the product's price, its availability, the name of the third-party seller, the time required to ship the product to the purchaser, and whether the third-party seller has paid Amazon to provide "fulfillment" services for the product. The seller's name is typically hyperlinked, so that prospective purchasers can access a separate webpage that lists other items sold by the seller, and reviewers of the seller submitted by other Amazon Marketplace users.

c. Product Reviews: The product page also includes a section that purports to summarize and excerpt product reviews submitted by other purported purchasers of the advertised product. More specifically, Amazon permits users of its marketplace to post product "reviews," which can include the reviewer's photographs of the product's features, a textual description of the product, and a "star-rating" of between 0 and 5 "stars" that correspond to the reviewer's satisfaction with the product. The product page provides information about the percentage of reviewers who have assigned particular "star" ratings to the product, and includes the full text of representative product reviews.

B. Background Regarding Amazon's Efforts To Regulate Amazon Marketplace

13. As the operator of Amazon Marketplace, Amazon regularly collects information about the sellers, products, and purchasers who participate in that marketplace. As Amazon's website explains, one of the ways in which Amazon uses this information is to regulate sellers, including by placing sellers on notice of purported delinquencies relating to their product offerings and/or by suspending sellers from further participation in the Amazon Marketplace. Based on my review of Amazon's website, and my interview of an Amazon representative familiar with Amazon's regulation of its Marketplace, the bases on which Amazon may discipline a seller are as follows:

(1) Deficiencies In Seller "Metrics":

14. Amazon collects "metrics" about seller performance, which it summarizes in the form of a rating called "Account Health." As Amazon's website explains, "Account Health" refers to a "seller account's adherence to the performance targets and policies

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

required to sell on Amazon." Amazon purports to "regularly review the performance of all sellers and notify them when they are off-target." Amazon's website also informs sellers that "[o]ccasionally, seller accounts with very poor performance are immediately deactivated."

15. Amazon collects certain "metrics" about sellers, and then compares those metrics to benchmarks. According to Amazon, the metrics that it collects include, but are not limited to, the following metrics:

a. Order Defect Rate: Amazon states that it tracks the percentage of defective "orders" within sixty-day periods. The term "defect" refers to "negative [customer] feedback" about the product, "an A-to-z Guarantee claim that is not denied,"[6] or a "credit card chargeback" by the purchaser. According to Amazon, an "Order Defect Rate" that is "above 1% may result in account deactivation."

b. Cancellation Rate: Amazon also monitors the percentage of completed product orders that sellers cancel during any given seven-day period. To be clear, these "seller-cancelled orders" are not cancellations initiated (or requested) by the purchasers, but instead are orders that the sellers elect to cancel. According to Amazon, its "policy is that sellers maintain a [cancellation rate] under 2.5% in order to sell on Amazon. A [cancellation rate] above 2.5% may result in account deactivation."

c. Late Shipment Rate: For orders in which the seller has not chosen to purchase Amazon's "fulfillment" services, Amazon tracks whether sellers ship the product in a timely manner. Specifically, Amazon tracks whether the date of confirmed shipment is "after the expected shipment ship date." Amazon states that its "policy is that sellers maintain [a late-shipment rate] under 4%" during any given 10- or 30-day period, and that a late-shipment rate of "above 4% can result in account deactivation."

---

[6] Amazon provides customers with an "A-to-z Guarantee" for certain categories of items. Under the guarantee, customers are eligible to request a refund directly from Amazon for items they purchase from third-party sellers if the delivery of the item is unduly delayed, the order is "different than expected," or the customer "returned [the] item with a trackable shipping method and the seller has not issued . . . a refund." *See* https://www.amazon.com/gp/help/customer/display.html?nodeId=201889410, *last accessed on* May 30, 2019 (3:47 p.m. PST).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(2) Amazon's Selling Policies And Seller Code Of Conduct

16. Amazon also requires third-party sellers on Amazon Marketplace to adhere to Amazon's "Selling Policies and Seller Code of Conduct" (hereinafter the "Code of Conduct"). According to Amazon, the penalties for noncompliance with the Code of Conduct can include account suspension.

17. The preamble to the Code of Conduct states that "[a]ll sellers are expected to adhere to the following policies when listing products on Amazon. Seller offenses and prohibited content can result in suspension of your Amazon account." The Code of Conduct elsewhere reiterates that "[v]iolation of the code of conduct principles may result in the loss of your selling privileges and removal from Amazon Marketplace."

18. Amazon's Code of Conduct includes several general "conduct principles," including that: (a) sellers "[a]dhere to all applicable laws and abide by all Amazon policies"; (b) "[n]ever misrepresent yourself"; (c) "[n]ever engage in any misleading, inappropriate or offensive behavior"; and (d) "[a]ct fairly at all times." These are not the only "conduct principles" that Amazon sets forth in its Code of Conduct, though these are the principles that have the greatest bearing on the conduct under investigation.

19. In addition to the general principles set out above, Amazon's Code of Conduct also sets forth certain specific policies. For instance, Amazon prohibits the listing of products where such listing would violate the law. Amazon also restricts the type of information that sellers may include on the product page, by prohibiting links to other external websites, requests by the seller for positive customer reviews, and promotional material regarding the seller.

20. Amazon also instructs sellers that "[a]ny attempt to manipulate ratings, feedback, or reviews is prohibited." Amazon, for instance, prohibits sellers from posting "abusive or inappropriate feedback . . . about a transaction partner," including by "posting ratings or feedback to your own account," or "pay[ing] or offer[ing] any incentive to a buyer for either providing or removing feedback." Amazon further instructs sellers that they "cannot review your own products or your competitor's products" or "ask a reviewer to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

change or remove their review." Amazon also prohibits sellers from taking steps to manipulate the algorithms that Amazon uses in order to track the number of visitors to product pages (which Amazon tracks in order to draw consumers' attention to "popular" or highly-trafficked products) – *e.g.*, by "simulating customer traffic."

(3) Adverse Commercial Consequences to Amazon Marketplace Sellers

21. As Amazon's representatives have explained to law-enforcement agents, sellers who participate in the Amazon Marketplace may suffer adverse commercial outcomes, or outcomes that fall short of their preferences. Such consequences may result from non-compliance with Amazon's various metrics and policies, including those described above. In such cases, Amazon often imposes the adverse consequence upon the seller after making its own determination about whether such non-compliance has occurred. Separately, sellers may suffer adverse consequences simply through the normal operation of the Amazon Marketplace, *e.g.*, because customers do not traffic their products frequently enough, causing their products to not feature prominently when customers search for such categories of products on the Amazon Marketplace.

22. For present purposes, the adverse consequences that sellers may face include: (a) Amazon's refusal to approve a certain product for sale on its Marketplace, e.g., because of concerns that it is counterfeit or dangerous; (b) Amazon's suspension of the sale of certain products; and (c) Amazon's suspension of a seller's ability to make any sales on Amazon Marketplace.

23. In the event that Amazon takes adverse action against a seller, the member of its seller-services or seller-enforcement team that takes such action typically notates an explanation of that adverse action in a computer system maintained by Amazon. Amazon refers to such internal notes as "annotations." The full "annotation history" regarding a particular third-party seller account reflects all of the notes taken by seller-services or seller-enforcement employees who have taken action with regard to a particular third-party seller account. In addition to these employee-created annotations, Amazon's servers may also automatically track activity taken with regard to third-party seller accounts, such as the name

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

of the employee who took the action, the date/time of that action, and (in some circumstances) certain information regarding the action taken.

24. Amazon may provide sellers with the opportunity to remedy the adverse consequences described above. Sellers typically are asked to submit a "Plan of Action" that describes the steps they plan to take in order to address the deficiencies in performance or compliance that resulted in the adverse action. One or more Amazon employees thereafter review the Plan of Action and take appropriate action in response to it (i.e., rejecting the seller's plan as inadequate, requesting additional information from the seller, or accepting the seller's plan). Sellers may also choose to appeal adverse consequences, including through so-called "escalations" to more senior employees at Amazon, including Amazon's Chief Executive Officer.

25. Based on my review of publicly available websites, I have learned that there is an industry of purported "consultants" who advise third-party sellers about maximizing their performance on the Amazon Marketplace. These consultants' websites state that their services include advising third-party sellers about how to respond to adverse actions taken by Amazon as a result of sellers' performance deficiencies and their failure adequately to comply with Amazon's policies. Some of the consultants identify themselves as former Amazon employees, who claim to have insight into how Amazon regulates third-party sellers and how sellers can persuade Amazon to reverse adverse consequences that may be imposed by Amazon.

C. **The Conduct Under Investigation**

26. In or about December 2018, Amazon reported to the FBI that some of its employees had admitted that they accepted commercial bribes from third-party Amazon Marketplace sellers, and that they favorably manipulated those sellers' accounts in exchange for those bribes.[7] According to Amazon, the employees' conduct was prohibited by the

[7] According to information provided by Amazon, the compromised employees were not employed by Amazon.com, Inc., but instead were employed by an Amazon-affiliated entity based in India named Amazon

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

terms of their employment agreements with Amazon. The conduct under investigation also violates various federal criminal laws.

27. According to Amazon, in the course of its internal investigation in the first half of 2018, its legal team interviewed and collected records from various Amazon employees who admitted to participating in the scheme described above. In the sections below, I set forth Amazon's description of its employee interviews and summarize the records that Amazon collected from those employees. In addition to the interviews described, some of the compromised Amazon employees also provided written statements to Amazon investigators that were substantively consistent with the accounts that they provided during their interviews.

28. As described further below, the Amazon employees who admitted to accepting commercial bribes in exchange for taking unauthorized action to benefit certain third-party sellers (referred to herein as the "compromised Amazon employees") reported that they undertook their unauthorized and unlawful conduct at the request of Joseph Nilsen ("NILSEN"), and NILSEN's associates. According to public-source records, including records maintained by the New York Secretary of State, NILSEN is a resident of New York and is the owner of Digital Checkmate Inc. ("Digital Checkmate"), a company registered in New York.

29. On the social-media website LinkedIn, NILSEN identifies himself as Digital Checkmate's Chief Executive Officer. NILSEN's profile page on the social-media website Quora claims that he is part of "an elite team" of "Amazon seller experts from all over the country" that is "unlike any other team that has ever existed." Nilsen asserts that this team "has already made history in several ways," by "combining collectively over 100 years of e-commerce experience, the most skilled programmers who have also been engulfed in the Amazon world for years, previous employees, data analyst and gifted writers."

[redacted]), or by third-party contractors retained by Amazon to perform seller-support services. For simplicity, this Affidavit refers to the employees as Amazon employees.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

30. Based on Amazon's interviews of the compromised Amazon employees, other records collected during the investigation, and public-records searches, I have determined that Digital Checkmate does business under the trade name "Seller Strategies." Digital Checkmate's website states that it offers an "elite team of Amazon seller consultants providing state-of-the-art e-commerce services for your marketplace success."[8] One of NILSEN's associates at Digital Checkmate is Kristen Michelle Leccese ("LECCESE"), who purports to serve as Digital Checkmate's Vice President. In her profile on the social-media website Quora, LECCESE identifies herself as a "Content Strategies and E-Commerce Consultant."[9] In addition, Leccese's publicly-accessible page on the social-media website Facebook advertises Digital Checkmate's services.

(1) Interview of [redacted]

31. According to Amazon, its legal department in India received a referral from Amazon's operational team in China regarding employee misconduct with respect to a seller account. The referral stated that a third-party seller on Amazon Marketplace named Buddibox harassed another third-party seller, which had submitted a confidential complaint about Buddibox to Amazon's seller-support team.

32. Through counsel, Amazon has confirmed that Buddibox was indeed a third-party seller on Amazon Marketplace at the time of the alleged misconduct (and thereafter). According to records maintained by the Secretary of State for Georgia, Buddibox LLC is an entity that has operated under the laws of the State of Georgia since July 2013. Its "organizer" and "registered agent" under Georgia law is Hadis Nuhanovic ("NUHANOVIC") and its principal place of business is in Acworth, Georgia.

33. According to Amazon, an investigation by its business team in China revealed that [redacted] an Amazon seller-support employee based in India, had checked the reporting seller's account, and therefore would have had access to

[8] *See* https://sellerstrategies.com, *last accessed on* June 10, 2019.
[9] *See* www.quora.com/profile/Kristen-Michelle-Leccese, *last accessed on* June 10, 2019.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

information about its complaint regarding Buddibox. Amazon's legal team interviewed [redacted] on or about August 29, 2018. During that interview, [redacted] confessed to Amazon that he shared proprietary information and took unauthorized official conduct to benefit Buddibox, all in exchange for approximately $14,500 in commercial bribes that Buddibox paid him. [redacted] told Amazon that a former Amazon colleague named Rohit Kadimisetty ("KADIMISETTY") introduced him to NUHANOVIC, and that he communicated with NUHANOVIC over WhatsApp at the phone number (404) 683-5737.[10] As described further below, emails produced by the compromised Amazon employees establish that KADIMISETTY is an associate of NILSEN's, who purports to act on NILSEN's behalf.

34. [redacted] asserted that NUHANOVIC asked [redacted] to use internal Amazon data for the following unauthorized purposes: (a) to optimize NUHANOVIC's advertising campaign, which [redacted] accomplished by changing product keywords in NUHANOVIC's seller account to improve sales performance; (b) to assist NUHANOVIC in marketing products in new product categories, by providing NUHANOVIC with proprietary information about the top-selling products in those potential product categories; and (c) to provide NUHANOVIC with product invoices, which NUHANOVIC used to create fake invoices. [redacted] further stated that, to facilitate this misconduct, NUHANOVIC provided [redacted] with access to NUHANOVIC's seller account, so that [redacted] could directly make beneficial changes to that account on the basis of Amazon's proprietary data. [redacted] also confessed that he uploaded proprietary Amazon data to NUHANOVIC's cloud-storage account.[11]

---

[10] Records produced by WhatsApp show that this phone number is registered to an email account that bears NUHANOVIC's first name.

[11] [redacted] told Amazon investigators that NUHANOVIC had a cloud-storage account hosted by Dropbox, Inc. ("Dropbox"), registered under the email address [redacted]gmail.com. Records produced by Google show that [redacted]gmail.com is registered under the name "[redacted] with a recovery e-mail address [redacted]@]yahoo.com. Records produced by Dropbox show that the cloud-storage account registered to [redacted]@]gmail.com was registered under the name "[redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

35. Records produced by MoneyGram – a money-transmittal service – show that NUHANOVIC made the following wire transfers to a MoneyGram user named [redacted]. In a WhatsApp chat, [redacted] told NUHANOVIC that [redacted] was his father, and instructed NUHANOVIC to wire the commercial bribes to his father, so that Amazon would not discover them:

Date	Amount (in U.S. Dollars)
April 13, 2018	2,000.00
April 17, 2018	1,100.00
April 25, 2018	1,000.00
May 15, 2018	2,000.00
June 17, 2018	3,700.00
July 19, 2018	2,747.00
August 22, 2018	1,500.00
October 18, 2018	500.00
November 21, 2018	800.00
December 4, 2018	880.00
December 21, 2018	800.00
January 24, 2019	1,000.00
February 23, 2019	1,000.00
March 21, 2019	1,250.00
April 20, 2019	1,350.00
May 24, 2019	1,000.00

36. Records produced by PayPal also show that, between January 2018 and March 2018, a PayPal account registered under the name "Buddibox LLC" and under NUHANOVIC's name made payments of $800.00 (on January 26, 2018), $315.00 (on March 1, 2018), $105.00 (on March 14, 2018), and $600.00 (on March 20, 2018) to a PayPal account registered to [redacted] under the email address [redacted]@]gmail.com.

37. [redacted] also told Amazon that he did similar work for other clients, who he met through KADIMISETTY.

(2) Interview of NISHAD KUNJU ("KUNJU")

38. [redacted] identified another Amazon employee named Nishad Kunju ("KUNJU") as a participant in the scheme described above. According to Amazon, KUNJU had the title of "Seller Support Associate" in Amazon's "Seller Brand Support" team. Amazon interviewed KUNJU on August 29, 2018.

39. According to Amazon, KUNJU admitted to accepting commercial bribes from NILSEN over the two years preceding the interview. According to KUNJU, NILSEN made

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

these commercial bribes on behalf of clients, including third-party sellers who had been referred to NILSEN by a law firm operating under the name [redacted][2]

40. KUNJU further claimed that he performed the following tasks, in exchange for the commercial bribes he received: (a) helping to reinstate suspended seller accounts by manipulating internal annotations, helping sellers prepare plans of actions, and escalating seller concerns; (b) sharing proprietary data about NILSEN's clients' (and their competitors') performance, disclosing the names of Amazon employees who could reinstate suspended seller accounts, and sharing Amazon's internal policies; and (c) providing commercial benefits to NILSEN's clients, by hampering their competitors' inventory, improving their own inventory, creating optimized product listings for them, and removing negative customer feedback.

41. KUNJU stated, and produced records showing, that he used the email address freakdaze[@]gmail.com to email with NILSEN and others associated with the scheme. In particular, KUNJU forwarded to Amazon's investigator over one-hundred emails that he sent or received at freakdaze[@]gmail.com. As set out below, these emails included numerous emails to/from NILSEN. According to KUNJU (and the records that he produced), NILSEN used the email addresses joe[@]digitalcheckmate.com and amazonnate11[@]gmail.com.

---

[12] According to its website, the law firm [redacted] operates under the brand name [redacted] *See* [redacted] *last accessed on*, June 6, 2019 (11:48 p.m. PST). KUNJU told Amazon investigators that NILSEN assigned KUNJU with tasks for clients of one of the attorneys at that law firm, who KUNJU identified as [redacted] website identifies its managing attorney as [redacted] *See* [redacted] *last accessed on* June 6, 2019 (11:52 p.m PST). KUNJU also claimed that he received commercial bribes from LECCESEE, who KUNJU also identified as associated with [redacted] Although the website for [redacted] does not list LECCESSEE as a member of that law firm, in a post submitted to the online message board Quora, a person named "Kristen Michelle Leccese" who identified herself as an "Amazon Seller Consultant & Content Writer" recommended "seeking a professional to help you get your account reinstated – check out [redacted] He is an attorney who focuses on Amazon sellers who have been suspended." *See* [redacted] *last accessed on* June 6, 2019 (12:01 p.m PST). LECCESE's page on the social-media website LinkedIn states that she is a Vice President at Digital Checkmate, Inc. ("Digital Checkmate") and an "Account Suspension Consultant" at Sellers Strategies International; it also states that she worked for Amazon Sellers Lawyers as an "account analyst" between March and September 2016. *See* https://www.linkedin.com/in/kristenmichelleleccese, *last accessed on* June 6, 2019.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

KUNJU also stated (and produced records showing) that he exchanged emails with KADIMISETTY at rogerparkin69[@]gmail.com.

42. Records produced by PayPal show that an account registered to NUHANOVIC made a $2,000.00 transfer to an account registered to "Nishad" under the email address freakdaze[@]gmail.com on or about June 9, 2018.

(3) Interview of [redacted]

43. Both [redacted] and KUNJU identified another Amazon employee named [redacted] as a participant in the scheme described above. According to Amazon, its legal department in India interviewed [redacted] on or about August 29, 2018. According to Amazon, [redacted] said that he had worked with NILSEN and KADIMISETTY to make changes to third-party seller accounts, in exchange for bribes. In particular, [redacted] said that NILSEN provided him with $12,000 in kickbacks in exchange for taking the following steps with regard to seller accounts: (a) making annotations relating to product listings or seller accounts that had been suspended or warned, with such annotations designed to improve the standing of those listings or sellers within the Amazon Marketplace; (b) changing product categories for clients' product listings, in order to drive sales; (c) sharing customers' email identifiers; (d) helping sellers with business and performance reports; (e) managing invoices relating to various sellers; and (f) sharing Amazon's confidential Standard Operating Policies.

44. [redacted] said that one of NILSEN's clients was a third-party seller that operated under the name [redacted] Amazon's website lists [redacted] seller identification number [redacted] told investigators that on NILSEN's instructions, [redacted] owner, who [redacted] identified by the name '[redacted]' paid [redacted] a monthly "salary" in exchange for [redacted] misuse of his

---

[13] *See* https://www.amazon.com/sp?seller=[redacted], *last accessed on* June 6, 2019. [redacted] produced an email to Amazon in which one of his colleagues, [redacted] sent him a "list" of product codes "that I have worked on." The subject line of that email was "Re: Seller ID: [redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

position at Amazon. [redacted] also produced email records showing that he used the email address [redacted]@]gmail.com to communicate with two [redacted] representatives, who used the addresses [redacted][@]gmail.com, [redacted]]gmail.com, and [redacted]@[redacted], as further discussed below. [redacted] also produced transcripts of WhatsApp chats that he had with a WhatsApp user named "[redacted] According to records maintained by the California Secretary of State, [redacted] is the registered agent of a Torrance, California corporation named [redacted] which was previously known as [redacted] Inc."

45. [redacted] admitted that he performed the following services for [redacted] and [redacted]: (a) disclosing and using proprietary Amazon information regarding other sellers' performance; (b) filing "refund" claims with Amazon on [redacted] behalf; (c) modifying [redacted] product listings to optimize performance, based on internal Amazon data.

46. [redacted] also produced emails showing that he used [redacted]@]gmail.com to communicate with NILSEN. In those exchanges, NILSEN used the email addresses jn[@]sellerstrategies.com, joe[@]digitalcheckmate.com, and amazonnate11[@]gmail.com. Emails produced by [redacted] also show that he corresponded with KADIMISETTY (who used the address rogerparkin69[@]gmail.com during those exchanges), and [redacted] (who used the address [redacted]@]gmail.com during those exchanges).

(4) Interview of [redacted]

47. Based on its review of internal data, Amazon identified another potentially compromised employee named [redacted] told Amazon's investigators that NILSEN had solicited him over Facebook, the social-media platform. [redacted] also admitted accepting commercial bribes from NILSEN in exchange for work that he performed for NUHANOVIC. [redacted] claimed that KADIMISETTY introduced him to NUHANOVIC. [redacted] also claimed that NUHANOVIC paid him

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

approximately $12,000 in commercial bribes in exchange for taking numerous acts that benefited Buddibox.

48. In particular, [redacted] told Amazon that he used Amazon's proprietary information to benefit Buddibox commercially. Specifically, [redacted] admitted that he helped write a "plan of action" that Buddibox presented to Amazon's seller-services department to forestall and overcome disciplinary action, informed Buddibox about the Amazon employees who had taken disciplinary action against Buddibox, and informed Buddibox about the customers who had negatively reviewed Buddibox products.

49. [redacted] also admitted that he checked on NUHANOVIC's account, by determining whether any listed products had been taken down (whether by error or otherwise) by Amazon. [redacted] further stated that NUHANOVIC gave him access to the Buddibox seller account, so that [redacted] could file various seller appeals on Buddibox's behalf.

50. [redacted] told Amazon that NUHANOVIC paid him over PayPal and MoneyGram. Records produced by MoneyGram show that NUHANOVIC sent the following payments to [redacted]:

Date	Amount (in U.S. Dollars)
January 23, 2018	450.00
February 7, 2018	700.00
February 28, 2018	625.00
March 7, 2018	500.00
March 24, 2018	200.00
April 9, 2018	1,500.00

51. NUHANOVIC also sent money to [redacted] over PayPal. Specifically, records produced by PayPal show that an account registered to NUHANOVIC made payments over $200.00 (on December 27, 2017) and $300.00 (on December 2, 2017) to a PayPal account registered to "[redacted] under the email address [redacted][@]gmail.com.

(5) Interview of [redacted]

52. Based on its review of internal data, Amazon identified another potentially compromised employee named [redacted] told Amazon's investigators that, in June 2018, a former Amazon employee called him and recruited him to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

participate in the conduct described above. After [redacted] agreed to the arrangement, the former Amazon employee introduced him to a third-party seller based in the United States named "[redacted] who used a WhatsApp account bearing the telephone number [redacted] to communicate with [redacted] Records produced by WhatsApp show that this number was registered with no identifying information (e.g., a name or email address).

53. [redacted] told Amazon that "[redacted] asked [redacted] to reinstate blocked sellers accounts, which [redacted] refused to do. According to [redacted] he did nonetheless agree to draft plans of action, which "[redacted] could present to Amazon's seller-support services in order to reinstate two blocked seller accounts. [redacted] admitted that he accepted $1,000 for each of those plans of actions, which resulted in the successful reinstatement of the two accounts at issue. [redacted] also claimed that the sender information on the payments revealed that the payments originated from NUHANOVIC, acting on behalf of Buddibox LLC. MoneyGram records show that NUHANOVIC made payments of $1,200 and $300 to K[redacted] on June 30, 2018 and July 15, 2018, respectively. In addition, a bank record that K[redacted] produced to Amazon shows that he received an $800 wire transfer from a JPMorgan Chase account registered under the name "Buddibox."

54. [redacted] produced email records showing that he used the email addresses [redacted]]gmail.com and [redacted]]gmail.com in connection with the conduct set out above.

D. Facts Establishing Probable Cause For Each SUBJECT ACCOUNT

55. As further described in each of the sub-sections below, probable cause exists to search each of the SUBJECT ACCOUNTS.

(1) amazonnnate11[@]gmail.com

56. As set out above, both KUNJU and [redacted] told Amazon that NILSEN used the email address amazonnate11[@]gmail.com when communicating with them in connection with the scheme. According to records produced by Google, amazonnate11[@]gmail.com was created on December 28, 2016 and terminated on August 31, 2018 (two days after Amazon interviewed a variety of compromised employees). Google's records also show that

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

amazonnate11[@]gmail.com exchanged emails with other accounts that Amazon employees identified as being used in connection with the scheme (as described further below), including kml[@]digitalcheckmate.com (used by LECCESE), joe[@]digitalcheckmate.com (used by NILSEN), and jn[@]sellerstrategies.com (used by NILSEN).

57. NILSEN identified amazonnate11[@]gmail.com in a WhatsApp chat with [redacted] (which [redacted] produced to Amazon). Specifically, when [redacted] asked NILSEN to "give me your email address so I can send you the annotations [regarding the third-party seller [redacted]]," NILSEN responded: "amazonnate11[@]gmail.com."

58. Emails produced to Amazon by [redacted] and KUNJU appear to show that amazonnate11[@]gmail.com sent and received numerous emails in furtherance of the suspected scheme.

a. ***First***, [redacted] and KUNJU exchanged emails with amazonnate11[@]gmail.com about the improper actions that they would take for NILSEN's clients in exchange for commercial bribes. For instance, on August 20, 2018, [redacted] and amazonnate11[@]gmail.com exchanged emails regarding a seller account operating under the trade name "[redacted] In that exchange, amazonnate11[@]gmail.com sent [redacted] a message saying "Here we go brother – I'll have more in the morning-mid afternoon as well. Just heating up. Please let me know if anything is unclear.' [redacted] responded that he was "able to remove feedback" for two orders but that he had been "informed that it is very risky to remove feedbacks," as a result of which he "cannot help in removing feedbacks as continuous audits are being removed."

[redacted] also turned over an email in which amazonnate11[@]gmail.com forwarded him a request from a third-party seller named [redacted] in which the seller asked NILSEN to "put this product ([redacted] in a specific product category on Amazon. In his email forwarding [redacted] request to [redacted] NILSEN stated: "They will send a TON of work. Whenever you bang something out you can just add it to Splitwise and when you call on the funds they will be ready and waiting." According to its website, Splitwise is an online tool through which people can track bills and share expenses.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Records produced by Splitwise show that NILSEN registered a Splitwise account under the name "Tom Jones," and registered the account using the email addresses joe[@]digitalcheckmate.com and amazonnate11[@]gmail.com

b. ***Second,*** [redacted] and KUNJU sent amazonnate11[@]gmail.com spreadsheets showing internal information stored by Amazon about third-party sellers. Amazon's records regarding each seller were contained in individual Microsoft Excel files with metadata showing that those files were created by the compromised employee who sent the information to NILSEN (i.e., [redacted] or KUNJU). The Microsoft Excel files typically contained three separate spreadsheets: (a) a spreadsheet named "Seller Information," which contained *inter alia* the seller's name, the number of products listed on Amazon, and the types of Amazon services utilized by the seller; (b) a spreadsheet named "Annotation history," which showed the most instances in which Amazon's seller-support team had taken specified types of actions with respect to the seller account (e.g., the date of the last email to the seller, the date of the last modification of the seller's inventory, and the date of the last modification to the seller's listings); and (c) a spreadsheet named "Annotations," which showed the date, content and internal notes regarding each Amazon seller-support action with respect to the seller account (as well as the name of the Amazon seller-support employee who took the action).

For instance, on August 29, 2018, [redacted] sent an email to amazonnate11[@]gmail.com that attached a Microsoft Excel file that disclosed Amazon's internal records regarding the third-party seller [redacted] The file contained an "Annotations" spreadsheet, which revealed to NILSEN that Amazon's seller-enforcement team had blocked [redacted] seller account because of food-safety issues and other product defects. Through counsel, Amazon has explained to the Government that the annotation history disclosed in these spreadsheets enabled NILSEN to craft a plan of action to help reinstate his clients' accounts, including by identifying the internal teams to target in any pleas for reinstatement.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

NILSEN also used amazonnate11[@]gmail.com to solicit information about particular products, on behalf of his clients. For instance, on or about July 18, 2018, KUNJU sent NILSEN "recon" about thirteen products, under the email subject line "Let's get this money & shut these fools up."

NILSEN also used amazonnate11[@]gmail.com to communicate with KADIMISETTY (at rogerparkin69[@]gmail.com), and then forwarded at least one such exchange to KUNJU. For instance, on or about January 30, 2018, amazonnate11[@]gmail.com forwarded an exchange that the account had with rogerparkin69[@]gmail.com about a client of NILSEN's who had been (potentially wrongfully) suspended by Amazon for selling infringing products. In the exchange, KADIMISETTY told NILSEN "If he pays 10 g's I am getting this account active." When NILSEN told KADIMISETTY that the seller intended to petition Amazon directly to lift the suspension, KADIMISETTY responded "Ask him to suck my dick.. lol. He ain't going anywhere without us." NILSEN and KADIMISETTY then exchanged emails debating the likelihood of the seller achieving a good result without their assistance.

c. ***Third***, KUNJU sent amazonnate11[@]gmail.com confidential Amazon information regarding "keywords" used by sellers on the Amazon Marketplace. As explained above, sellers can provide Amazon with certain "keywords" that associate with particular products for sale, so that purchasers who search for those keywords on the Amazon Marketplace will see the sellers' products among search results for those keywords. KUNJU shared information about the frequency with which prospective customers searched for particular keywords—information that would have enabled NILSEN's clients to provide Amazon with keywords that increased the likelihood of their products appearing among the search results seen by purchasers. For instance, on or about July 23, 2018, KUNJU emailed amazonnate11[@]gmail.com a document named "top_keyword.csv" that contained extensive data regarding keyword searches for particular categories of products.

d. ***Fourth***, KUNJU sent amazonnate11[@]gmail.com confidential Amazon information regarding its seller-enforcement policies. For instance, on or about July

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

13, 2018, KUNJU sent amazonnate11[@]gmail.com an email that attached a document named "Notes." The document's metadata reflected that it was created by KUNJU, and the text of the document purported to reflect internal notes from Amazon to its seller-support team regarding the procedures for approving certain products for sale on the Amazon Marketplace. The document contained the note "***INTERNAL INFORMATION – DO NOT SHARE WITH THE SELLER***" As another example, on or about July 20, 2018, KUNJU sent amazonnate11[@]gmail.com several Amazon documents, including documents that set forth Amazon's seller-enforcement policies, and sent an email to amazonnate11[@]gmail.com on August 24, 2018 with attachments about Amazon's policies regarding the protection of intellectual property rights. In addition to sharing such documents with amazonnate11[@]gmail.com, KUNJU also sent an email to amazonnate11[@]gmail.com about the mathematical formula that Amazon used in its algorithm to rank customer reviews regarding products.

e. ***Fifth***, amazonnate11[@]gmail.com sought input from KUNJU with regard to drafts of emails to Amazon that NILSEN created on his clients (i.e., third-party sellers on Amazon Marketplace) behalf. The draft emails purported to petition Amazon to take favorable action with respect to the client's seller account on Amazon Marketplace. In light of the statements made by KUNJU and other Amazon employees during their interviews, I submit that there is probable cause to believe that NILSEN sought KUNJU's input on these draft emails because he expected that KUNJU could apply proprietary Amazon information to improve the draft emails' likelihood of causing Amazon to take favorable action with respect to the third-party sellers' accounts. KUNJU also sent a draft Plan of Action to amazonnate11[@]gmail.com on January 21, 2018, so that NILSEN's client could submit that draft to Amazon's seller-support services.

f. ***Sixth***, KUNJU and amazonnate11[@]gmail.com exchanged emails regarding fund transfers from NILSEN to KUNJU. For instance, on or about May 21, 2017, KUNJU emailed NILSEN to confirm *inter alia* that he had made the following changes with respect to a product listing on the Amazon Marketplace: "Changed the main image to the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

secondary image for the ASIN [redacted] NILSEN responded by stating that he "[w]ill certainly pay for whatever was done." Similarly, on or about June 11, 2017, using amazonnate11[@]gmail.com, NILSEN emailed KUNJU to note that "I just wanted to reach out and apologize about the funds not getting transferred right away. I did not know that Rohit wanted me to send them how I just did." Further, in a November 2017 email chain in which KUNJU pointed out ways in which NILSEN could reduce the cost of selling products on Amazon through NILSEN's own seller account (named "[redacted] KUNJU referred to a promise from KADIMISETTY that "my pay would be 1250/month."

g. ***Seventh***, in various emails, KUNJU and NILSEN referred to ways in which NILSEN's own business could improve its sales and profitability on the Amazon Marketplace. KUNJU identified product numbers for NILSEN to procure and sell, and provided NILSEN with data about product categories. In such emails, KUNJU and NILSEN referred to KUNJU as an ostensible member of this business, even though KUNJU was employed by Amazon.

(2) joe[@]digitalcheckmate.com

59. As set out above, KUNJU and [redacted] both identified the email address joe[@]digitalcheckmate.com as an account that NILSEN uses in connection with the criminal scheme. Records produced by Google show that joe[@]digitalcheckmate.com is an email account administered by Google (under a custom domain name chosen by the subscriber, as an alternative to the default "@google.com" or "@gmail.com). The subscriber name on the account is "Joe Nilsen." In addition to email, the joe[@]digitalcheckmate.com account also receives Google Docs, Google Drive, and Google Voice services.

60. The records produced by Google establish probable cause to search joe[@]digitalcheckmate.com for email content, as further described in Attachment B-1 below. Connection records produced by Google show that joe[@]digitalcheckmate.com exchanged nearly four thousand emails with email accounts associated with Amazon seller services, including [redacted][@]amazon.com and [redacted][@]amazon.com.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

joe[@]digitalcheckmate.com also communicated with LECCESE at kml[@]digitalcheckmate.com.[14]

61. In addition, emails produced by [redacted] and KUNJU show that NILSEN used joe[@]digitalcheckmate.com in furtherance of the scheme under investigation:

a. ***First***, as with amazonnate11[@]gmail.com, NILSEN used joe[@]digitalcheckmate.com to receive Microsoft Excel spreadsheets that contained internal Amazon data regarding seller accounts. For instance, on or about August 26, 2018, [redacted] (using [redacted][@]googlemail.com) sent an email to joe[@]digitalcheckmate.com under the subject line "Annotation for [redacted] A Microsoft Excel spreadsheet attached to the email contained information about a third-party seller on Amazon Marketplace operating under the trade name "[redacted]."

b. ***Second***, NILSEN used joe[@]digitalcheckmate.com to solicit input from compromised Amazon employees about how his clients could petition Amazon to take actions that benefited them. For instance, on or about August 22, 2018, NILSEN forwarded KUNJU an email that NILSEN received from LECCESE (at kml[@]digitalcheckmate.com) with the subject line "[redacted] The email contained a draft communication to Amazon, petitioning Amazon to lift a suspension on a seller account. The draft communication was signed "[redacted] Founder and CEO, [redacted]." According to records maintained by the Secretary of State for New York, [redacted] is the registered agent of a company named [redacted], which (according to Amazon records) operates under the trade name "[redacted]" on the Amazon Marketplace. On or about August 28, 2018, NILSEN sent a message over WhatsApp to [redacted] in which he stated: "Remember I told you I'd let you know if I have somebody willing to pay more for a particular service? This guy is looking for annotations. [redacted] The one request he had is that they go back to at least July 1st. He is willing to pay 500. 250/each?"

[14] According to records produced by Google, the address kml[@]digitalcheckmate.com is registered to "Kristen Michelle."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

According to Amazon's website, the seller identification number "[redacted] corresponds to "[redacted]." According to emails he produced to Amazon, KUNJU received two emails from PayPal confirming that [redacted] sent KUNJU $250.00 and $300.00 in March and June 2018.

c. ***Third***, NILSEN used joe[@]digitalcheckmate.com to receive emails regarding the payment of commercial bribes to compromised Amazon employees. For instance, on or about July 22, 2018, the online money-remittance service Remitly sent an email to joe[@]digitalcheckmate.com confirming the electronic transfer of 136,420.00 Indian Rupees to [redacted] NILSEN proceeded to forward the email from Remitly to KUNJU.

d. ***Fourth***, NILSEN used joe[@]digitalcheckmate.com to instruct other members of his organization: Seller Strategies. For instance, in or about July 2018, NILSEN exchanged emails with an individual named [redacted] (who used the email address "[redacted]sellerstrategies.com"). [redacted] sent NILSEN an email under the subject line "PAYONEER,"[15] which stated: "Please resubmit the request. I will have to do it manually with them. I spent 6 hours working on this this afternoon." NILSEN responded by instructing [redacted] to send funds to a purported Philippines resident named [redacted]" using Remitly.

62. There is also probable cause to search joe[@]digitalcheckmate.com for Google Voice records associated with the account, including stored voicemails, transcripts of stored voicemails, and text messages received and sent by the account. Records produced by Google show that the Google Voice number associated with the account is ([redacted] Connection records produced by Google show that NILSEN used Google Voice to send and receive numerous "SMS" messages and audio calls, and that he received voicemails at the account. The telephone numbers from which NILSEN received voicemails and with which

[15] According to its website, Payoneer is an online money-transfer service.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

he exchanged SMS text messages include telephone numbers bearing the country code for India (+91).

(3) jn[@]sellerstrategies.com

63. There is also probable cause to search the Google account registered under jn[@]sellerstrategies.com. Subscriber records produced by Google show that jn[@]sellerstrategies.com is registered to "Joe Nilsen." Emails produced by [redacted] show that NILSEN used jn[@]sellerstrategies.com in connection with the scheme, by receiving the client request referred to above at jn[@]sellerstrategies.com and then forwarding that request to amazonnate11[@]gmail.com.

64. KUNJU also produced an email to Amazon investigators showing that NILSEN used jn[@]sellerstrategies.com in connection with the scheme. Specifically, on or about August 13, 2018, jn[@]sellerstrategies.com forwarded to KUNJU an email that he received from a company named "[redacted] that purported to offer services similar to those offered by NILSEN's company. In the email, a representative of [redacted] told NILSEN that "[w]e unblock almost any banned [seller] to receive new reviews ASIN, allowing you to get within 24H, a brand-new listing page that will allow you to start sell again and collect new reviews without any removals of inventory or any other action on your side!"

65. WhatsApp chats produced by compromised Amazon employees also show that NILSEN used jn[@]sellerstrategies.com in connection with the scheme. In two emails attached to a WhatsApp chat in which NILSEN referred to unauthorized action on behalf of a client named [redacted] NILSEN (at jn[@]sellerstrategies.com) received emails from B[redacted] regarding Amazon's "denial" of [redacted] plan of action regarding the suspension of its account for violating Amazon's terms of service.

66. Connection records produced by Google also show that NILSEN used jn[@]sellerstrategies.com in connection with the scheme. Using jn[@]sellerstrategies.com, NILSEN exchanged more than 9,000 emails with Amazon seller-services email accounts, and there is probable cause to believe that such emails will reflect the identities of NILSEN's clients and the actions that he sought to take on their behalf. NILSEN also used

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Jn[@]sellerstrategies.com to exchange emails with others (e.g., employees) associated with his business, who used the email addresses [redacted]@]sellerstrategies.com, [redacted] b[redacted]@]sellerstrategies.com, [redacted]@]sellerstrategies.com, [redacted]]sellerstrategies.com, b[redacted]@]sellerstrategies.com, [redacted]@]sellerstrategies.com, [redacted]@]sellerstrategies.com, [redacted]@]sellerstrategies.com, n[redacted]@]sellerstrategies.com, [redacted]@]sellerstrategies.com, [redacted]@]sellerstrategies.com, b[redacted]@]sellerstrategies.com, and [redacted]@]sellerstrategies.com.

(4) [redacted]]gmail.com

67. There is also probable cause to search the Google account registered under [redacted]@]gmail.com. Records produced by Google establish probable cause to believe that [redacted]@]gmail.com was used by [redacted][16] who B[redacted] KUNJU, and [redacted] identified to Amazon investigators as a former Amazon employee who had taken a position working for NILSEN.

68. KUNJU provided Amazon investigators with a transcript of a WhatsApp chat that he had with [redacted] regarding unauthorized action with respect to Amazon seller accounts. In one chat, [redacted] asked KUNJU: "[redacted] – *Account suspended. Can we get it reinstated?*" [redacted] also provided Amazon investigators with spreadsheets showing activity in his bank account as "proof of receipt of money" from N[redacted] (in addition to [redacted] and KADIMISETTY). The spreadsheet showed debits of 50,000 Indian Rupees, 80,000 Indian Rupees, from "[redacted]" on or about May 23, 2018 and June 28, 2018 respectively.

69. KUNJU also provided Amazon investigators with a February 1, 2018 email that he sent to both NILSEN and [redacted]@]gmail.com (as a carbon copy recipient) saying "[w]e shud be able to do it. If seller has request approval button then it's done," with regard to a client inquiry that NILSEN had forwarded to KUNJU.

---

[16] For instance, [redacted]]gmail.com has the same recovery phone number as [redacted] [redacted]]gmail.com and [redacted]@]gmail.com.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

70. Connection records produced by Google show that [redacted]gmail.com exchanged emails with an account registered to Amazon seller services: [redacted][@]amazon.com. Those connection records also show that joe[@]digitalcheckmate.com exchanged approximately thirty emails with [redacted]gmail.com, and that kml[@]digitalcheckmate.com exchanged approximately three emails with [redacted]gmail.com

(5) kml[@]digitalcheckmate.com

71. There is also probable cause to search the Google account registered to kml[@]digitalcheckmate.com. Records produced by Google show that that this account is registered to "Kristen Michelle"—i.e., LECCESE's first and middle names. As set out above, in at least one email, LECCESE used kml[@]digitalcheckmate.com to send a draft email to NILSEN on behalf of a NILSEN client named [redacted]. In addition, Google connection records show that kml[@]digitalcheckmate.com exchanged with other email addresses used in furtherance of the scheme, including joe[@]digitalcheckmate.com (more than 1,000 emails), and jn[@]sellerstrategies.com (more than 100 emails), and x[@]digitalcheckmate.com (15 emails).

(6) [redacted]yahoo.com, [redacted]gmail.com, freakdaze[@]gmail.com, [redacted]googlemail.com, [redacted]gmail.com, [redacted]gmail.com, [redacted][@]gmail.com, [redacted][@]gmail.com (collectively "Compromised Employee Accounts")

72. There is also probable cause to search the Compromised Employee Accounts—i.e., the email accounts used by the Amazon employees who have admitted to participating in the criminal scheme under investigation. Much of the probable cause relating to each of the Compromised Employee Accounts already has been set out above. The following bullets summarize those facts and provide additional factual information for accounts that have not already been addressed above.

a. [redacted]yahoo.com and [redacted]gmail.com: As set out above, [redacted] used [redacted]gmail.com to register a PayPal account,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

at which he received commercial bribes from NUHANOVIC. [redacted] produced multiple emails showing his use of [redacted]@]gmail.com in furtherance of the scheme, including several emails from PayPal confirming the transmission of payments by Buddibox or NUHANOVIC, and an email from Dropbox confirming that [redacted] had been given access to Buddibox's Dropbox account by NUHANOVIC. [redacted] also produced the transcript of a WhatsApp chat that he had with a user named "Hadis" (i.e., Hadis Nuhanovic), in which [redacted] stated that he one or more documents for NUHANOVIC were "uploading on google drive bro." Moreover, [redacted] sent emails to Amazon investigators using [redacted]@]yahoo.com, to which he attached files containing proprietary Amazon data regarding customer orders, which [redacted] apparently compiled for NILSEN.

b. freakdaze[@]gmail.com: As set out above, KUNJU admitted that he used freakdaze[@]gmail.com in furtherance of the criminal scheme, and produced emails to Amazon showing that he used that account to correspond with NILSEN (at amazonnate11[@]gmail.com) and KADIMISETTY (at rogerparkin69[@]gmail.com) about seller account annotation histories, seller inventories, and the optimal ASIN under which to categorize products for sale on Amazon Marketplace. Furthermore, in WhatsApp chats, KUNJU told NILSEN that he could receive funds from NILSEN and his clients at a PayPal account registered to freakdaze[@]gmail.com.

c. [redacted]]googlemail.com: As set out above, [redacted] produced emails showing that he used the email address [redacted]@]googlemail.com to communicate with NILSEN and NILSEN's clients, in connection with misusing his position at Amazon in exchange for commercial bribes. The emails produced by [redacted] show that he stored documents associated with the scheme in his cloud-storage account (through the service Google Drive), which also was registered under the email address [redacted]@]googlemail.com. For instance, [redacted] provided Amazon investigators with a screenshot of multiple emails that he referred to as a "Print screen of the link of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Google drive shared," in which he sent [redacted] (at [redacted][@]gmail.com) access to various files.

d. [redacted]@]gmail.com, [redacted]@]gmail.com: As set out above, [redacted] told investigators that he used these two email addresses in furtherance of the scheme. [redacted] also produced emails showing that: (i) his bank in India sent emails to [redacted]]gmail.com confirming the transmission of funds to him by Buddibox; and (ii) he used [redacted]]gmail.com to communicate with an "outsider" (in his words) to whom he provided services by misusing his access privileges at Amazon; in the emails, [redacted] provided drafts of emails and letters that the third-party seller could send to Amazon in order to reverse adverse action taken by Amazon against the third-party seller's account.

e. [redacted][@]gmail.com: Emails produced by KUNJU show that KUNJU delegated some of the work he performed for NILSEN's clients to an Amazon employee named [redacted] Using the email address [redacted][@]gmail.com, [redacted] collected and sent KUNJU internal Amazon information about its seller-management systems, including with regard to account suspensions and intellectual-property issues. In discussions with the government, Amazon has characterized this type of material as proprietary and potentially consisting of trade secret information in certain circumstances. After she was approached by Amazon investigators, [redacted] turned over emails that she had received at [redacted]gmail.com from HDFC Bank Limited (a bank based in India) alerting her to activity relating to her account.

f. [redacted][@]gmail.com: Emails produced by [redacted] show that [redacted] delegated some of the work he performed for NILSEN's clients to an Amazon employee named [redacted]"). On or about July 15, 2018, using the email address [redacted][@]gmail.com, [redacted] sent [redacted] two emails, which [redacted] had produced to Amazon, in which she: (i) provided a "list of below UPCs that I have worked on," followed by a list of product codes; and (ii) shared a Microsoft Excel

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

spreadsheet listing several internal Amazon transaction numbers relating to customer-refund requests for items that had been "damage[d] in transit."

(7) ellekaye11[@]gmail.com

73. There is also probable cause to search ellekaye11[@]gmail.com. Records produced by Google show that ellekaye11[@]gmail.com was registered to under the name "KM Elle." The records also show that the account is related by SMS (i.e., it shares the same recovery telephone number) as other accounts bearing Kristen Leccese's initials (i.e., "KML").

74. Connection records produced by Google, which do not reflect the content of email messages but do reflect the email addresses on either side of the transmission (and the date of such transmission), establish probable cause to believe that elleykaye11[@]gmail.com may contain evidence of the crimes under investigation, including evidence about the identity of the user of joe[@]digitalcheckmate, which (as explained above) was used in connection with the scheme under investigation. Those records show that, on or about August 31, 2018, elleykaye11[@]gmail.com received an email from joe[@]digitalcheckmate.com.

(8) rogerparkin69[@]gmail.com

75. There is also probable cause to search rogerparkin69[@]gmail.com. As explained above, KUNJU stated (and produced records showing) that KADIMISETTY used rogerparkin69[@]gmail.com in connection with the suspected criminal scheme. The records produced by KUNJU include the email referred to above between NILSEN and KADIMISETTY, which NILSEN forwarded to KUNJU.

76. Subscriber records produced by Google show that the person who registered rogerparkin69[@]gmail.com did not provide any name at the time of registration. However, connection records produced by Google show that the user of rogerparkin69[@]gmail.com exchanged other emails associated with the scheme (as described elsewhere in this Affidavit), including [redacted][@]gmail.com, kml[@]kristenleccesse.com, joe[@]digitalcheckmate.com, and [redacted]@]gmail.com during the time period under investigation.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

77. In addition, both [redacted] and KUNJU produced emails showing that KADIMISETTY used rogerparkin69[@]gmail.com in connection with the criminal scheme. In several of those emails, the name associated with rogerparkin69[@]gmail.com was "Roger Park." For instance, [redacted] produced the following emails showing that he corresponded with rogerparkin69[@]gmail.com in connection with the scheme:

a. On or about August 19, 2018, [redacted] sent rogerparkin69[@]gmail.com a spreadsheet with the file name "Orders," which contained a list of hundreds of orders for a particular product (including customer email addresses associated with those orders).

b. On or about August 1, 2018, [redacted] engaged in an email exchange with rogerparkin69[@]gmail.com, in which KADIMISETTY responded to [redacted] delivery of information regarding product orders by promising to "find out the money transfer process and send it to you."

c. On or about July 29, 2018, [redacted] sent rogerparkin69[@]gmail.com a spreadsheet with the file name "306FifthAveCharity." The spreadsheet contained a detailed history about Amazon's internal actions over time with respect to a seller account operated by [redacted].

d. On or about July 29, 2018, [redacted] sent rogerparkin69[@]gmail.com a spreadsheet with the file name "New list of email." The spreadsheet contained a list of orders for a particular product (including customer email addresses associated with those orders).

e. On or about August 1, 2018, [redacted] sent rogerparkin69[@]gmail.com an email that attached two documents containing detailed histories about Amazon's internal actions over time with respect to the seller accounts operated by [redacted] and [redacted]

f. On or about July 28, 2018, [redacted] sent rogerparkin69[@]gmail.com an email that attached a document containing a detailed history of Amazon's internal actions

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

over time with respect to a seller account. The file name of the spreadsheet was "[redacted]

g. On or about July 23, 2018, rogerparkin69[@]gmail.com sent [redacted] an email stating "Add 450 to the Tab."

78. KUNJU also exchanged emails with rogerparkin69[@]gmail.com in connection with the scheme. For instance:

a. Between on or about March 28, 2017 and March 29, 2017, KUNU and rogerparkin69[@]gmail.com exchanged emails under the subject line "Suspended accounts." In that exchange, KUNJU initially provided rogerparkin69[@]gmail.com with what he characterized as "data for suspended accounts. The data only has 22 of them." Using rogerparkin69[@]gmail.com, KADIMISETTY responded: "Bro… Please try to finish it "as soon as possible". I have sent it to them, try to complete now." Later in the exchange, KUNJU sent KADIMISETTY what he characterized as the "Remaining data."

b. On or about November 16, 2017, KUNJU sent rogerparkin69[@]gmail.com the annotation history for an Amazon Marketplace seller named "[redacted]

c. On or about June 29, 2018, KUNJU sent rogerparkin69[@]gmail.com an email attaching an invoice for multiple products that had been issued by an apparent wholesaler of those products. As explained above, in some circumstances, Amazon requires third-party sellers to produce invoices to show that they obtained their products from a registered wholesaler.

(9) [redacted][@]gmail.com and [redacted]@]gmail.com (collectively the "[redacted]")

79. There is also probable cause to search [redacted][@]gmail.com, and k[redacted]]gmail.com, based on evidence that these two accounts were used by a third-party Amazon seller named [redacted]" in connection with the criminal scheme under investigation. As explained above, [redacted] told Amazon investigators that he provided information to a representative of [redacted] named

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

[redacted] also identified [redacted]gmail.com and [redacted]. (This application does not seek authority to search [redacted]

80. Subscriber and connection records produced by Google establish that:

a. [redacted][@]gmail.com was registered under the name "[redacted] and that it is linked by SMS (i.e., it shares a recovery telephone number) with [redacted]gmail.com.[17] Between in or around 2013 and in or around August 2018, the account exchanged approximately 50,000 emails with addresses bearing the domain name "amazon.com," which tends to establish that the account was used to communicate regarding a seller account on Amazon Marketplace.

b. [redacted]gmail.com was registered under the name [redacted]." Between in or around 2013 and in or around August 2018, [redacted]gmail.com exchanged emails with an Amazon.com email address associated with Amazon's seller-services unit.

81. Records produced by [redacted] show that the [redacted] Accounts were used in connection with the scheme. For instance:

a. On or about August 26, 2018, [redacted]gmail.com forwarded to [redacted] an email that all three of the [redacted] Accounts had received from a member of Amazon's Seller Support team. The underlying email referred to [redacted] query regarding Amazon's decision to refund one of its customers for an item, purportedly because of the customer's claim that the item had been "damaged in transit."

b. On or about August 18, 2018, [redacted] sent [redacted][@]gmail.com and [redacted]gmail.com an email

[17] According to records produced by Google, the email address [redacted]gmail.com is registered to "[redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

with the subject line "[redacted] reports." The email attached an archive file (or ".zip" file) named "[redacted] The archive contained files that displayed inventory information and sales information for a variety of products. Similarly, on or about July 13, 2018, [redacted] sent [redacted][@]gmail.com an email with the subject line "[redacted] [redacted] which contained similar inventory and sales information.

(10) NILSEN's Facebook Account

82. There is also probable cause that NILSEN's Facebook Account will contain evidence of the crimes under investigation. [redacted] told Amazon that NILSEN approached him over Facebook and offered him the opportunity to make "easy money." Subscriber records produced by Facebook show that an account bearing account number 557853344 is registered to "Joe Nilsen," and bears the vanity name "joenilsenseo." The registered email addresses associated with the account are joe[@]digitalcheckmate.com and ellekaye11[@]gmail.com.

83. Connection records produced by Facebook establish probable cause to believe that NILSEN's Facebook Account was used to communicate with clients, compromised Amazon employees, and NILSEN's associates.[18] For instance:

a. Between 2017 and February 2019, NILSEN exchanged dozens of messages with a Facebook user named [redacted]

b. Between July 2018 and February 2019, NILSEN exchanged several messages with a Facebook user named "[redacted]." According to Amazon's website, a seller named [redacted] operates on Amazon Marketplace under seller identification number [redacted] According to emails he produced to Amazon, [redacted] sent internal data regarding [redacted] seller account to rogerparkin69[@]gmail.com on or

[18] Facebook produced connection records for NILSEN's Facebook Account in response to an Order issued by the United States District Court for the Western District of Washington. The connection records reveal the dates, times, and counterparties to communications sent from and received by NILSEN's Facebook Account, but the records do not reveal the content of any such communications.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

about July 14, 2018. As with the other spreadsheets described above, the internal data reflected Amazon's internal annotations.

c. Between 2017 and 2019, NILSEN exchanged messages with a Facebook user named "Hadis Nuhanovic." As explained above, records produced by [redacted] records produced by MoneyGram, and connection records produced by Google show that NUHANOVIC paid commercial bribes to Amazon employees, in exchange for which those employees took favorable actions with respect to the Buddibox account on Amazon Marketplace.

d. Between 2014 and 2019, NILSEN exchanged hundreds of messages with a Facebook user named "Kristen Michelle" (with the Facebook account number 23004459). According to records produced by Facebook, the user "Kristen Michelle" registered their Facebook account using the email address kristenleccese[@]gmail.com. As explained above, the compromised employees' statements and records, as well as publicly-available records, establish that LECCESE is an executive at Digital Checkmate, who has arranged for the payment of commercial bribes to Amazon employees, in exchange for which those employees took favorable action for Digital Checkmate's clients.

e. Between 2017 and 2018, NILSEN exchanged messages with a Facebook user named [redacted]." According to records maintained by the Secretary of State for Texas, [redacted] is the registered agent for a third-party seller on Amazon Marketplace named "[redacted]." Amazon's website shows that [redacted] operates under the seller identification number [redacted]. Records produced by [redacted] to Amazon show that on or about July 1, 2018, [redacted] sent an email to rogerparkin69[@]gmail.com, which attached a spreadsheet named "[redacted]," containing internal Amazon data regarding [redacted] account. On or about September 4, 2018, NILSEN sent KUNJU messages over WhatsApp, in which he requested information and input about how [redacted] could respond to adverse action by Amazon with respect to its seller account. NILSEN, in particular, sent KUNJU a draft email to Amazon from [redacted] which purported to be signed by "[redacted]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Owner – [redacted]." When KUNJU offered to draft a Plan of Action that [redacted] could present to Amazon, NILSEN accepted the offer, but also noted that "I am not taking a penny from this guy."

(11) LECCESE's Facebook Account

84. There is also probable cause that LECCESE's Facebook Account will contain evidence of the crimes under investigation. As explained above, subscriber records produced by Facebook show that an account bearing account number 23004459 is registered to "Kristen Michelle," and bears the vanity name "kaymichelle." The registered email address associated with the account is kristenleccese[@]gmail.com. As explained above, there is probable cause to believe that kristenleccese[@]gmail.com is LECCESE's email account, and that it is an instrumentality of the crimes under investigation.

85. Connection records produced by Facebook establish probable cause to believe that LECCESE's Facebook Account was used in furtherance of the scheme under investigation. More specifically:

a. Between 2017 and February 2019, LECCESE exchanged hundreds of messages with [redacted]. As explained above, [redacted] is associated with [redacted], a third-party seller on the Amazon Marketplace, and sent commercial bribes to KUNJU (according to records produced by KUNJU).

b. Between 2017 and February 2019, LECCESE exchanged approximately one hundred messages over Facebook with Hadis Nuhanovic. As explained above, records collected over the course of the investigation establish that Nuhanovic is a principal at Buddibox who paid commercial bribes to Amazon employees in exchange for favorable treatment with respect to the Buddibox seller account.

c. Between 2017 and February 2019, LECCESE exchanged dozens of messages with a Facebook user named "Rohit Gupta." According to [redacted] "Rohit Gupta" was an alias used by KADIMISETTY in the course of the scheme under investigation. In addition to exchanging messages directly with "Rohit Gupta," Leccese

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

also participated in a Facebook "chat" through which Nilsen, Leccese, and "Rohit Gupta" all exchanged messages among one another.

d. Between 2017 and February 2019, LECCESE participated in multiple chats with Nilsen and representatives of Amazon Marketplace sellers. I have developed probable cause that the third parties to these chats were representatives of those sellers by searching for their names in publicly-available databases, and tracing that information back to the Amazon Marketplace. In addition, as explained above, between 2014 and 2019, Leccese exchanged hundreds of Facebook messages with Nilsen.

e. Between 2017 and February 2019, LECCESE exchanged hundreds of messages with a Facebook user named "Ed Rosenberg." As explained above, Rosenberg is a partner at the law firm [redacted]. According to KUNJU, NILSEN purported to refer Rosenberg's clients to KUNJU, and those clients paid commercial bribes in exchange for favorable treatment for their Amazon Marketplace accounts. In one WhatsApp chat produced by KUNJU, KUNU purported to send a message he received from NILSEN to [redacted] in which NILSEN asked for information about a third-party seller account, noting that "Ed involved and it's important to keep good relations with him."

(12) SELLER STRATEGIES' Facebook Account

86. There is also probable cause that Seller Strategies' Facebook Account will contain evidence of the crimes under investigation. As explained above, subscriber records produced by Facebook show that an account bearing account number 607905026066065 with the vanity name "sellerstrategies" was created by LECCESE on or about June 21, 2006. The registered email address associated with the account is kristenleccese[@]gmail.com. As explained above, there is probable cause to believe that kristenleccese[@]gmail.com is LECCESE's email account, and that it is an instrumentality of the crimes under investigation.

87. Connection records produced by Facebook establish probable cause to believe that LECCESE's Seller Strategies Facebook Account was used in furtherance of the scheme under investigation. More specifically:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Between 2017 and 2019, Seller Strategies exchanged messages with a Facebook user named [redacted] under the Facebook user identification number [redacted] The Facebook page for that user contains a link to the Facebook seller page for [redacted]" a third-party seller operating on the Amazon Marketplace.

b. In 2018, Seller Strategies exchanged messages with a Facebook user named [redacted] registered under the Facebook user identification number [redacted] The Facebook page for that user refers to a company named [redacted] which (according to Amazon's website) is a third-party seller operating on Amazon Marketplace.

c. In 2018, Seller Strategies exchanged messages with a Facebook user named [redacted] registered under the Facebook user identification number [redacted] According to his publicly available profile on the social-media website LinkedIn, [redacted] is a Manager at a Florida company named [redacted] LLC. According to Amazon's website, [redacted] LLC is a third-party seller operating under the trade named [redacted] on the Amazon Marketplace.

d. In 2018, Seller Strategies exchanged messages with a Facebook user named "[redacted] registered under the Facebook user identification number [redacted] According to his publicly available profile on the social-media website LinkedIn, [redacted] is a "Category Head" at a company based in India named [redacted] According to Amazon's website, [redacted] is a third-party seller on the Amazon Marketplace.

(13) Apple iCloud Accounts Bearing Digital Sign Identifiers 10075071322 And 1712170805

88. There is also probable cause to believe that Apple iCloud accounts bearing the digital sign identifiers ("DSID") numbers 10075071322 and 1712170805 will contain evidence, fruits, and instrumentalities of the crimes set out above.

89. According to records produced by Apple, DSID number 1712170805 ("NILSEN's iCloud account") has been registered to joe[@]digitalcheckmate.com since

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

March 1, 2013. As set out above, joe[@]digitalcheckmate.com is registered to "Joe Nilsen," and was used by NILSEN in furtherance of the scheme.

90. According to records produced by Apple, DSID number 10075071322 ("LECCESE's iCloud account") has been registered to kristenleccese[@]gmail.com since November 30, 2015. As set out above, kristenleccese[@]gmail.com was used by LECCESE to register Facebook accounts in her name and in Seller Strategies' name. In addition, records produced by Google show that kristenleccese[@]gmail.com was registered under the name "Kristen Michelle," and that it shared a common recovery email address with kml[@]digitalcheckmate.com. As set out above, LECCESE used kml[@]digitalcheckmate.com in furtherance of the scheme under investigation.

91. Logs of activity on LECCESE's iCloud account and NILSEN's iCloud account for all such periods of time for which such logs are available (i.e., for the time period May 6 to May 16, 2019) show that both accounts utilize the iCloud "Backup" service. According to Apple's website, "iCloud Backup makes a copy of the information on your iPhone, iPad, and iPod touch." Apple's website further states that the data backed up by the iCloud backup product includes "iMessage, text (SMS), and MMS messages," as well as "photos and videos on your iPhone, iPad, and iPod touch." iCloud backup also saves a user's "App data" to their remote storage; in my training and experience, I am aware that such app data can include the contacts on a user's Apple iPhone, which can serve as evidence of the individuals who they know and the extent to which they have been in contact with those people – facts that can evidence the existence of a conspiracy.

92. The app data backed up by the iCloud backup program also can include the contents of WhatsApp chats, including attachments shared in those chats. Here, records produced by WhatsApp show that both NILSEN and LECCESE used WhatsApp from Apple devices under telephone numbers associated with their Apple iCloud accounts. More specifically:

a. **NILSEN**: Records produced by WhatsApp show that an account registered to the telephone number (212) 251-0100 uses the screenname "Joe" and most

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

recently has accessed WhatsApp using an Apple iPhone XS. When registering his iCloud account, NILSEN provided the telephone number (212) 251-0100.

b. **LECCESE**: Records produced by WhatsApp also show that a WhatsApp account has been registered to the telephone number (917) 854-0262. Those records also show that the account was most recently accessed using an Apple iPhone X. When registering her iCloud account, LECCESE provided a different telephone number. However, LECCESE provided the telephone number (917) 854-0262 at several points in time between 2016 and the present when logging into related Apple services, like Apple iTunes, and when purchasing devices from Apple.

93. Based on the facts set out above—*i.e.*, the use of iCloud backup, the registration with WhatsApp, the installation of WhatsApp on Apple iPhones, and the link between the telephone numbers used to register the WhatsApp accounts and the telephone numbers used in connection with Apple services—I respectfully submit that there is probable cause that LECCESE's iCloud account and NILSEN's iCloud account contain the transcripts of WhatsApp chats, including the attachments used in those chats.

94. There is also probable cause that LECCESE and NILSEN used WhatsApp in furtherance of the crimes under investigation, and that the contents of the WhatsApp chats found in their iCloud accounts will serve as evidence of those crimes. As set out above, the compromised Amazon employees told Amazon investigators that they used the encrypted online messaging application WhatsApp in connection with the scheme. BHOWMICK, KUNJU, and ELISHA provided Amazon investigators copies of those chats, which Amazon subsequently produced to the government. The WhatsApp chats show that NILSEN and LECCESE used the WhatsApp accounts registered under the telephone numbers (212) 251-0100 and (917) 854-0262 respectively to communicate with each other and with compromised Amazon employees about misusing their authority to benefit third-party Amazon sellers in exchange for commercial bribes. More specifically:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. *NILSEN's Use of WhatsApp*

95. Both [redacted] and KUNJU produced transcripts of their WhatsApp chats with NILSEN. In those chats, NILSEN used the WhatsApp screenname "Joe." In addition to producing a transcript of his WhatsApp chat with NILSEN, KUNJU also produced the transcript of a WhatsApp "group chat," whose participants included NILSEN, LECCESE, and KUNJU. According to KUNJU, NILSEN established the group chat, and assigned a name to the group chat of "100% only Reinstatement." As Amazon representatives have explained, and as documents in the investigation show, the term "reinstatement" is a term commonly used within Amazon to refer to third-party seller accounts that previously were suspended and later were "reinstated" by a member of Amazon's seller-support team.

96. The chat transcript produced by [redacted] included messages that [redacted] and NILSEN exchanged between July 30, 2018 and August 29, 2018. "Joe" initiated that chat on or about July 30, 2018 by stating: "[redacted] --- what's going on bro? Pleasure to finally have the ability to communicate with you." "Joe" told [redacted] that he wanted to "talk to you and see what abilities you have and how we can work together." In the chat, NILSEN sent [redacted] a link to a shared-file on the Google Drive platform, which NILSEN claimed to have created in order to set forth the "prices" for services apparently offered by NILSEN's consulting firm. NILSEN told [redacted] that "I deal with an insane amount of sellers daily" and that "the majority of the orders I place through you are not actually for me, and neither you nor I are doing these things because these people are our friends or we have fun doing it. We are doing it to make money." Over the remainder of the WhatsApp chat, NILSEN solicited [redacted] to use his access privileges at Amazon to take favorable actions for NILSEN and/or his clients, including by disclosing clients' annotation histories, removing negative customer feedback regarding clients, modifying category listings for clients' products to improve the profitability of product sales, sharing metrics about high-volume sellers, collecting data regarding reimbursements owed by Amazon to third-party sellers, and sharing information about competing Amazon sellers. NILSEN promised [redacted] "a tremendous amount of work for you, if you desire to take it on," and [redacted] responded "I

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

am ready to take up the work. Pricing we can negotiate. The more work the less I will charge." NILSEN also made repeated references to sharing files that he stored in his Google Drive folder with [redacted]

97. The chat transcripts produced by KUNJU included messages that [redacted] and NILSEN exchanged between April 3, 2018 and August 30, 2018. The chat transcript takes up approximately 500 pages. Throughout the chat, NILSEN asked KUNJU to misuse his position at Amazon to benefit NILSEN's clients, including by potentially recruiting other Amazon employees to accept commercial bribes. For instance, in an April 12, 2018 exchange, NILSEN informed KUNJU that a client's products had been blocked, and KUNJU told NILSEN to "strike a deal" with the client and to tell the client that "we will try to use the loop holes and get it done."[19] Later that day, NILSEN discussed recruiting current and former Amazon employees to serve his clients, stating "I feel like we just need as many soldiers as possible in there. Any department – any bullshit – handled." NILSEN further explained: "They do not get paid a great deal of money. I mean, there is no way we can be dishing out thousands to everyone. But if someone in category approval team bangs out 5 DVD approvals for us and you toss them like a 1k we just made 24k with no bullshit."

98. In addition to asking KUNJU to take action on behalf of his clients, NILSEN also asked KUNJU to misuse his position in connection with NILSEN's own third-party sellers account on Amazon Marketplace. For instance, in late April 2018, KUNJU shared Amazon's internal metrics regarding product sales with NILSEN, and informed NILSEN that "non-hazmat" products (e.g., nail clippers) performed well on the Amazon Marketplace. NILSEN, in turn, asked KUNJU to examine information that other third-party sellers provided Amazon, in order to identify the wholesalers from whom those sellers had purchased the products.

---

[19] Approximately seven days later, NILSEN confirmed that the client had agreed to pay "$9,500" for the job, which included reinstating certain suspected product listings, "reviews are back to how they were," and "ensuring they don't get taken back within a short amount of time," over all of which the client requested a "45 day guarantee."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. *LECCESE's Use of WhatsApp*

99. KUNJU also produced transcripts that establish LECCESE's use of WhatsApp in furtherance of the scheme. In a chat with KUNJU that took place between April 3, 2018 and April 4, 2018, LECCESE used the WhatsApp screenname "Kristen." As set out above, KUNJU also produced the transcript of a group chat, consisting of KUNJU, NILSEN, and LECCESE, in which LECCESE also used the screenname "Kristen." In both chats, LECCESE and KUNJU discussed KUNJU's misuse of his authority at Amazon to benefit third-party sellers, in exchange for commercial bribes

100. For instance, in a chat between KUNJU and LECCESE, LECCESE asked KUNJU "[w]hat's easiest for you and I to coordinate," in an apparent reference to tasks that KUNJU could perform on behalf of LECCESE's clients. KUNJU responded: "Storage limit increase, hazmat, ungating, feedback removal." (As Amazon representatives have explained, "ungating" is a term commonly used to refer to the process by which Amazon screens certain products before they can be sold on the Amazon Marketplace – e.g., by requiring sellers to provide proof that they purchased the product(s) from a bona fide wholesaler and that the product is not counterfeit.) LECCESE responded: "Un gating OK I was going to say that's what they always want." LECCESE later asked KUNJU: "What's the going rate for category and feedback," to which KUNJU responded: "We are charging 3k for topicals" and "Feedback it's 100." LECCESE stated that she would "play dumb and add a few hundred anywhere I can." KUNJU and LECCESE also exchanged messages about a third-party seller client who had asked for the removal of negative product reviews regarding counterfeit items that they were selling on the Amazon Marketplace.

101. In the group chat between KUNJU, LECCESE, and NILSEN, LECCESE repeatedly referred to KUNJU's misuse of his authority in exchange for commercial bribes. The chat addressed the suspension of a seller account operated by a seller named B[redacted] NILSEN shared documents that contained [redacted] Plan of Action, its appeal for reinstatement, and Amazon's denial [redacted] selling privileges. LECCESE also sent a link to a Google Drive file that contained a plan of action that

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

purportedly addressed a similar concern faced by another client, stating "Joe, here is the seller's 1st and 2nd attempts and our successful POA for the same issue recently. T- - i will share this link to you also, if you need it, its here, and my outline will be here as well." The three members of the chat eventually agreed to petition Amazon to reinstate the client's seller account by attributing the client's suspension to activity that a freelancer took on its behalf.

(14) Quora Accounts Registered To NILSEN and LECCESE

102. There is also probable cause to search accounts that NILSEN and LECCESE have registered on the social-media website www.quora.com. According to its website, Quora is an online social-media platform that enables users to post questions that can be answered by "people who really understand the issues and have first-hand knowledge." Based on my review of Quora's website, I am aware that registered users can maintain a "profile page" that sets out their name, photograph, and other biographical information that they provide. Users can post questions to the broader community of Quora users and can answer questions posed by those users. Based on an internal algorithm that appears to account for Quora users' qualifications, the depth of their responses, and the extent to which Quora users have engaged with their responses, Quora ranks responses to questions.

103. There is probable cause to believe that both NILSEN and LECCESE have used Quora to network with other Quora users, and to share their views regarding the operation of third-party seller accounts on Amazon. By reviewing the Quora website, I learned that NILSEN maintains a profile in which he refers to himself as a "Senior Amazon Strategist," as reflected by the screenshot below:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



Joe Nilsen
Senior Amazon Strategist
>>>Seller Strategies International

I am here to offer any insight I may have on particular topics and learn from some of the brilliant minds that occupy Quora.

Professionally, I am currently working with some of the brightest and most experienced people in the world regarding e-commerce, particularly on the Amazon.com platform.

Amazon seller experts from all over the country have come together to build an elite team that is unlike any other team that has ever existed. By combining collectively over 100 years of e-commerce experience, the most skilled programmers who have also been engulfed in the Amazon world for years, previous employees, data analyst and gifted writers, this team has already made history in several ways.

104. Connection records produced by Google establish probable cause to believe that NILSEN's Quora account is registered under joe[@]digitalcheckmate.com. Specifically, on multiple dates between in or about September 2018 and in or about December 2018, joe[@]digitalcheckmate received emails from email addresses bearing the "@quora.com" domain name, and which appear to be auto-generated emails from Quora. Some of those emails were sent by the address "messages-noreply[@]quora.com," which in my training and experience is an email signifier that social-media companies use when sending emails informing a user that he/she has received a message from another user of the social-media platform.

105. I also have learned that LECCESE operates an account on Quora. In her Quora profile, a screenshot of which appears below, LECCESE refers to herself as a "Content Strategist & E-Commerce Consultant."



Kristen Michelle Leccese
Content Strategist & E-Commerce Consultant

Be smart, be strong, be proud. Live honorably and with dignity, and just hold on.

It was #checkmate before the first pawn ever moved.

www.KristenLeccese.com

106. Connection records produced by Google establish probable cause to believe that LECCESE's Quora account is registered under kristenleccese[@]gmail.com and kml[@]digitalcheckmate.com. Specifically, between in or about March 2018 and in or about

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

December 2018, kristenleccese[@]gmail.com and kml[@]digitalcheckmate.com received multiple emails from email addresses bearing the domain name "@quora.com."

107. There is also probable cause to believe that the contents of messages that NILSEN and LECCESE have posted on Quora, and their exchanges with other users on the Quora network, will provide information about the consulting business that they operate, the types of clients they purport to serve, and the manner in which they attempt to benefit third-party sellers on the Amazon Marketplace. For instance, my review of Quora's website shows that NILSEN has supplied answers to a number of questions posed by other Quora users about the Amazon Marketplace, including "How serious is Amazon's fake review problem?," "What are the best tools to use to promote a new e-Business?," "How do I get bestsellers rank on Amazon.com?," "How long my Amazon seller account under review?," and "What are some extremely black hate tactics that Amazon FBA sellers are using?" For instance, in his response to the last question quoted above, NILSEN stated:

> I have no problem answering this question, but please understand that I am aware of these tactics because I am in the industry, not because I practice them. Ohhh the ways the people try to get over on Amazon and their search algorithm – it is insane. Had these people placed their attention and hard work into something legitimate, they would be far more successful and be socially accepted. But, they didn't, so here we are. Some of these tactics are not a drastic surprise, however, the lengths some go to are quite shocking.

NILSEN proceeded to embed a video and provided text description of steps that third-party sellers (and those sellers' agents) took in order to manipulate Amazon's algorithms.

108. LECCESE likewise has posted responses to Quora users' questions about the Amazon Marketplace, such as "Are there any successful Amazon sellers out there who would be willing to guide me as I select my first product?," and "How many products did you have to add to your Amazon business before you were able to support yourself financially full time?" In her responses, LECCESE purported to share information about how best to manage sales on Amazon Marketplace.

109. Indeed, on or about July 13, 2018, LECCESE submitted the following post on Quora's website bearing the title "How Amazon is Forcing Fair Sellers to Fight Dirty." The

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

tactics described in LECCESE's post are consistent with the tactics that NILSEN and his clients asked the compromised Amazon employees to undertake in exchange for commercial bribes, as reported by those employees and as evidenced by the emails and WhatsApp chats that those employees provided to Amazon's investigators. The post purports to describe how, because of Amazon's purported efforts to regulate activity on the Amazon Marketplace, "Fighting Dirty is Forced – Not Optional."

110. Although the contents of NILSEN's and LECCESE's public postings on Quora are available to anyone who browses to Quora's website, some of the information relating to their accounts can only be obtained through a search warrant. Such information includes the users who "follow" NILSEN and LECCESE—*i.e.*, the users who keep track of their posts and questions—as well as the users who NILSEN and LECCESE follow. Nor are any private messages that NILSEN and LECCESE exchanged with other Quora users publicly available. I respectfully submit that, in light of NILSEN and LECCESE's use of the Quora platform to share their views about commercial success on the Amazon Marketplace, there is probable cause to believe that information about their followers, the individuals who they follow, and the contents of messages they share with other Quora users is likely to evidence the crimes under investigation.

(15) LinkedIn Account Registered To NILSEN

111. There is also probable cause to search an account registered to NILSEN on the social-media website LinkedIn, under the vanity name "joenilsenseo." The vanity name "joenilsenseo" is the same vanity name that NILSEN has used for his Facebook account. Based on my review of LinkedIn's website, I have learned that NILSEN maintains a profile on LinkedIn, which can be accessed on the website https://www.linkedin.com/in/joenilsenseo (last accessed on July 18, 2019). The profile identifies NILSEN as "Joe N." a "CEO at Digital Checkmate Inc." based in New York, NY. The profile also includes the same photograph of NILSEN that appears on NILSEN's profile on Quora. In his LinkedIn profile, NILSEN claims that he has various skills, including "Selling on the Amazon Marketplace."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

112. The public version of NILSEN's LinkedIn profile shows that he has authored several posts (which are linked to on his LinkedIn profile) regarding optimizing sales performance on Amazon Marketplace. The titles of NILSEN's posts on LinkedIn include "Amazon Has Lost Control of Their Product Reviews," "Amazon Seller Feedback – How to Step Your Game Up," and "Why Every Amazon Seller Should Study The Movie American Gangster." In one those posts, NILSEN stated that "[t]he methods sellers use to obtain false reviews have increased in complexity. Many buyers would be appalled to hear what sellers do to get such high numbers of reviews."

113. In transcripts of WhatsApp chats produced by the compromised Amazon employees, NILSEN referred to his use of LinkedIn to scout out potential Amazon employees who he could bribe. For instance, in a chat on or about June 12, 2018, NILSEN engaged in the following exchange with KUNJU:

> [12/05/18, 10:52:47 AM] Joe: Yeah internal team my buddy has on his side as well --- it's these people that keep knocking stuff out ... You know I'm nuts though. I actually found them
> [12/05/18, 10:52:50 AM] Joe: https://www.facebook.com/[redacted]
> [12/05/18, 10:53:36 AM] Joe: Accenture <---- this is the company Amazon outsources to
> [12/05/18, 10:56:35 AM] Kunju: Did u contact him?
> [12/05/18, 11:05:01 AM] Joe: Noo..I just found these guys ... I am trying to find them all on [redacted] and Facebook and watch them for a few days. This is so important --
> Can't be screwed up. You can learn a lot about a person by what they post on social media or where they "check in" ect. After I get a general idea of character profiles, need to decide if it's best to hire somebody from over there to approach them and set up a call or just straight up reach out. If I just straight up reach out they are very skeptical and sometimes just won't respond
> [12/05/18, 11:06:04 AM] Kunju: If they are Indians I can pitch in for you.
> [12/05/18, 11:07:00 AM] Joe: I don't want to place your job at risk though .... I just want to do it the safest way possible with the highest chance of success
> [12/05/18, 11:07:51 AM] Kunju: I'll create a fake profile and contact them. Only if u need me to pitch in
> [12/05/18, 11:08:26 AM] Joe: Oh shit yeah dude if you can do so without being detected absolutely

114. Similarly, in an August 1, 2018 exchange, NILSEN told KUNJU that he planned to offer "2k to any legit soldiers that are recruited," and further stated that he "scraped linkedin for the members of teams I know we need. Then, we utilized custom

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

searches to find them on Facebook." NILSEN proceeded to state that several Amazon employees who he approached "will never talk to me," surmising that they suspected that he was an Amazon representative who was testing their vulnerability to commercial bribery ("I don't blame them. Amazon always pulling some slick shit.").

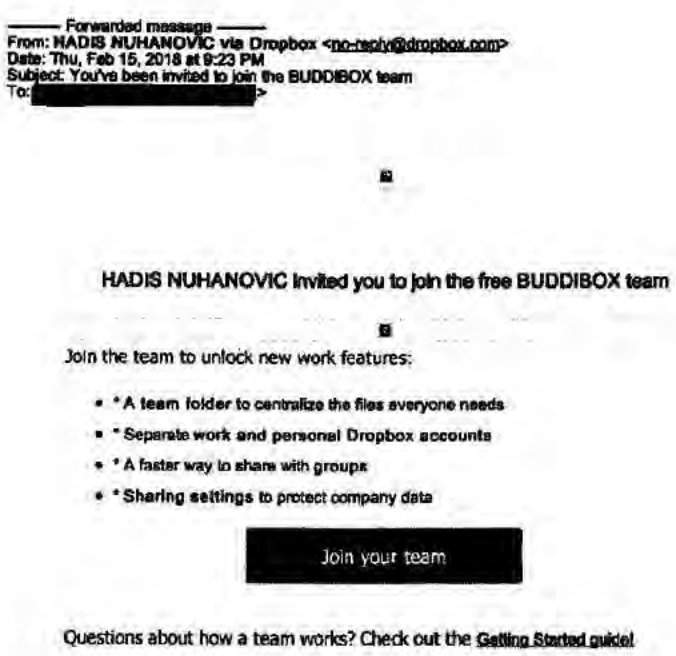
115. Based on these facts, I respectfully submit that records regarding NILSEN's activity on LinkedIn, such as his browsing history on the platform, and the messages he exchanges with other LinkedIn users, will evidence the crimes under investigation.

(16) Dropbox Accounts Accessed By [redacted]

116. There is also probable cause to search a cloud-storage account hosted by Dropbox, Inc. ("Dropbox"), which [redacted] accessed in the course of the scheme. When interviewed by Amazon investigators, [redacted] explained that NUHANOVIC provided [redacted] with access to a cloud-storage account on Dropbox, so that the two men could exchange electronic material that [redacted] prepared for NUHANOVIC, in exchange for the commercial bribes he received from NUHANOVIC. [redacted] stated that he used his email address–[redacted]gmail.com—to log into the Dropbox account that NUHANOVIC created for him. Records produced by Dropbox establish that the B[redacted] email was used to log into a Dropbox account on February 15, 2018, February 19, 2018, and November 6, 2018.

117. Emails produced by [redacted] confirm his account that he accessed and logged into a Dropbox account to which NUHANOVIC provided him access. In a February 15, 2018 email (i.e., the same day that Dropbox records show [redacted] logging into Dropbox), Dropbox sent an auto-generated email to [redacted] as follows:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



——— Forwarded message ———
From: HADIS NUHANOVIC via Dropbox <no-reply@dropbox.com>
Date: Thu, Feb 15, 2018 at 9:23 PM
Subject: You've been invited to join the BUDDIBOX team
To: [redacted]>

HADIS NUHANOVIC invited you to join the free BUDDIBOX team

Join the team to unlock new work features:

- * A team folder to centralize the files everyone needs
- * Separate work and personal Dropbox accounts
- * A faster way to share with groups
- * Sharing settings to protect company data

Join your team

Questions about how a team works? Check out the Getting Started guide!

118. Two minutes later, Dropbox sent another email to [redacted] "welcome[ing]" him to Dropbox. In my training and experience, the second email was an auto-generated email sent by Dropbox after [redacted] successfully accepted the invitation to join Buddibox's Dropbox account in the earlier email.

BACKGROUND REGARDING EMAIL SERVICE PROVIDERS

119. In my training and experience, I have learned that Google and Yahoo provide a variety of on-line services, including electronic mail ("email") access, to the general public. Google provides subscribers email and chat accounts at the domain names "[@]gmail.com" and "[@]googlemail.com." Yahoo provides subscribers email accounts at the domain name "[@]yahoo.com."

120. Subscribers obtain an account by registering with Google and Yahoo. When doing so, the email providers ask the subscriber to provide certain personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

investigation because the information can be used to identify the account's user or users, and to help establish who has dominion and control over the account.

121. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. As with subscriber records, IP address information can help to identify which computers or other devices were used to access the email account, which in turn can be used to identify the account's user or users, and to help establish who has dominion and control over the account.

122. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation, because the information can be used to identify the account's user or users.

123. In general, an email that is sent to a subscriber is stored in the subscriber's "mail box" on the email provider's servers until the subscriber deletes the email. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to the provider's servers, and then transmitted to its end destination. The email provider often maintains a copy of received and sent emails. Unless the sender specifically deletes an email from the email provider's server, the email can remain on the system indefinitely. Even if the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

subscriber deletes the email, it may continue to be available on the email provider's servers for some period of time.

124. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by the email provider but may not include all of these categories of data.

125. In addition to email and chat, Google and Yahoo offer subscribers numerous other services including:

a. **Google**: (i) Google Chrome Sync, which transposes a Google user's internet bookmarks, browsing history, and passwords to all devices they log into using their Google account name and password; (ii) Google Drive, which allows users to store documents and other files on remote servers operated by Google; (iii) Location History, which saves information about the physical locations of devices logged into a Google account; and (iv) Web & Activity, which saves information about Google web searches and browsing activity conducted by a user logged into a particular Google account.

b. **Yahoo**: Yahoo collects certain location information related to Yahoo account holders. On Yahoo's webpage under "Yahoo Privacy Policy," Yahoo had informed users that it may collect account holders' location information such as: (i) Pinpointed Physical Location, which collects physical location information from technologies like GPS, Wi-Fi, or cell tower proximity, upon a user's consent; (ii) Locations Entered, which collects location information that a user searches for, adds, or otherwise provides to Yahoo; (iii) IP Address information, which relates to device location; (iv) Partner Location Information, which relates to location data that Yahoo receives from third parties with whom a user has linked accounts. Users may opt out of the collection and storage of such location information by Yahoo, as well as the provision of that information by Yahoo to commercial third parties (such as app developers). Thus, if the user of SUBJECT ACCOUNT 17 utilized a mobile device to access the account and did not disable location services on their device(s)

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

or through their Yahoo account settings, Yahoo may have detailed records of the locations at which the account holder(s) utilized their mobile devices.

126. Based upon my training and experience, all of the types of information set out in the preceding paragraph may be evidence of the crimes under investigation in this case. As explained above, records produced by the compromised Amazon employees establish that one of the features of the scheme was the disclosure and use of proprietary Amazon information to benefit third-party sellers on Amazon Marketplace, and the corresponding disclosure of information from the third-party sellers (and their agents) in relation to the services they wanted the compromised Amazon employees to perform. For instance, as described above, [redacted] and [redacted] produced emails showing that they shared links to files stored in Google Drive with [redacted] and NUHANOVIC respectively. Similarly, in the WhatsApp chats described above, both NILSEN and LECCESE referred to files they had saved in Google Drive regarding the work they needed KUNJU and/or other compromised Amazon employees to perform on behalf of their clients.

127. There is also probable cause to believe that the web browsing history and Google Chrome Sync records for SUBJECT ACCOUNTS 1 through 16 will contain evidence the crimes under investigation. As set out above, in emails and WhatsApp chats, the perpetrators of the scheme referred to products sold on Amazon Marketplace and sellers on that marketplace—information that they derived by accessing Amazon's website. Evidence about their browsing history can therefore help identify the clients on whose behalf the compromised Amazon employees acted and the products with respect to which they took such action.

128. There is also probable cause to believe that the locations of the users of SUBJECT ACCOUNTS 1 through 17 will serve as evidence of the crimes under investigation. Evidence about the users' location can tie the accounts to particular individuals. In addition, because the scheme involved compromised Amazon employees who abused their positions of trust and access privileges in exchange for commercial bribes, the locations of those employees at the time they communicated with NILSEN and NILSEN's

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

clients can shed light on whether the employees accessed Amazon's computer networks from Amazon's office space or from other (remote) locations.

129. Both Google and Yahoo are also able to provide information that will assist law enforcement in identifying other accounts associated with SUBJECT ACCOUNTS 1 through 17, namely, information identifying and relating to other accounts used by the same subscribers. This information includes any forwarding or fetching accounts[20] relating to SUBJECT ACCOUNTS 1 through 17, all other accounts linked to those SUBJECT ACCOUNTS because they were accessed from the same computer (referred to as "cookie overlap"), all other accounts that list the same SMS phone number as those SUBJECT ACCOUNTS, all other accounts that list the same recovery email addresses[21] as do those SUBJECT ACCOUNTS, and all other accounts that share the same creation IP address as those SUBJECT ACCOUNTS. Information associated with these associated accounts will assist law enforcement in determining who controls those SUBJECT ACCOUNTS and will also help to identify other email accounts and individuals relevant to the investigation.

BACKGROUND REGARDING FACEBOOK

130. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

131. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical

---

[20] A forwarding or fetching account related to either SUBJECT ACCOUNT would be a separate email account that can be setup by the user to receive copies of all of the email sent to the account.

[21] The recovery email address is an additional email address supplied by the user that is used by the email provider to confirm a username after an email account's creation, help the user if the user is having trouble signing into their account, or alert the user to any unusual activity involving the user's email address.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

132. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

133. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

134. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

135. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

136. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

137. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

138. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

139. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

140. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

141. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

142. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

143. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

144. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

145. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

146. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

147. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner.

148. Facebook account activity may also provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

149. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

BACKGROUND REGARDING APPLE ID AND iCLOUD[22]

150. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

151. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

---

[22] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

152. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

153. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

154. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

155. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

156. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

157. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

158. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. For instance, evidence that identifies the user of an Apple iCloud account at the time that the phone connected to that account engaged in a WhatsApp chat (or sent an email) can establish a direct connection between the phone's user and the incriminating chat (or email).

159. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. In this case, as explained above, records produced by the compromised Amazon employees establish that multiple records connected to NILSEN and LECCESE's Apple iCloud accounts serve as evidence of the crimes under investigation, including WhatsApp chats backed up to those iCloud accounts and documents saved to their devices for use in connection with the scheme.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

160. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

161. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

162. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation, including the identities of third-party sellers who participated in the scheme and the products they sold on Amazon Marketplace.

163. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

BACKGROUND REGARDING QUORA

164. "Quora" is a social-networking website operated by Quora Inc. that can be accessed from any device with a connection to the internet. To become a member of Quora's online community, a user must register on Quora's website, www.quora.com. Quora requires its users to be at least thirteen years old at the time of registration, and to provide their real name (rather than a pseudonym or screenname).

165. Quora purports to allow users to post questions to the broader community of Quora users, and to respond to questions posed by other users. According to Quora's Terms of Service, "[t]he Quora Platform enables you to add posts, texts, photos, videos, links, and files to share with others." Although only Quora's registered users can post and respond to questions, the material that they post "may be viewed by the general public." According to Quora, its "platform offers a place to ask questions and connect with people who contribute unique insights and quality answers."

166. Quora collects and retains information about its users' activity on the Quora platform, including the information they provide at the time of registration, including their "name, contact information, and other information, such as topics that you know about or find interesting." Quora also retains the photograph that a user may elect to provide at the time of registration, so that other users can identify them by their photograph (in addition to their real name). In my training and experience, there is probable cause that such information may serve as evidence of the crimes under investigation by helping to identify the users of Quora accounts that have been used in furtherance of the crime. Here, for instance, information that NILSEN and LECCESE provided at the time of registration can establish a link between those individuals and their account activity.

167. Quora also collects and retains information about users' "content," which Quora defines to include "questions, answers, photos, and comments." Quora also collects "metadata" regarding such content, including "date and time stamps" associated with such

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

content. (Such information is publicly available.) As explained above, there is probable cause to believe that the content of NILSEN and LECCESE's posts on Quora establish that both individuals were involved in the business of consulting with third-party sellers on Amazon Marketplace, and that they were aware of the illicit conduct in which compromised Amazon employees engaged at their direction.

168. Quora also collects and retains information about communications between its users and with Quora's administrators. In my training and experience, such communications serve as additional attribution evidence to help identify the specific individual who is using a Quora account.

169. Quora also collects and retains "linked network" information regarding its users. Specifically, Quora's website states that "[y]ou can elect to sign in or sign up to the Quora Platform through a linked network (i.e. Facebook or Google), and you can connect your existing Quora account with certain third party networks like Facebook, Twitter and LinkedIn." Quora collects and retains information that those linked networks provide to Quora at the time that a user establishes a connection between their Quora account and their account on one of those networks; such information can include "certain profile and account information" supplied by the linked network provider. In my training and experience, such linked network information can serve as additional evidence about the actual identity of a Quora account's user.

170. Quora also collects and retains evidence about a user's activity on the Quora platform, including "cookies, log files, pixel tags [*e.g.*, electronic labels assigned to certain images that relate to the user], local storage objects," and other information like "searches, page views, date and time of your visit." In this case, evidence about NILSEN and LECCESE's activity on Quora's network can evidence the clients they sought to solicit, and the Amazon-based advice they solicited.

171. Quora also collects and retains information that a user's device may transmit to Quora regarding "browser type, type of computer or mobile device, . . . IP address, . . . [and]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

unique device identifier." In my training and experience, such information can further identify the precise individual who used a Quora account.

BACKGROUND REGARDING LINKEDIN

172. "LinkedIn" is a social network operated by LinkedIn, Inc., a subsidiary of Microsoft Corporation. Like Facebook, LinkedIn is an online community that registered users can access from any internet-connected digital device.

173. LinkedIn collects and retains certain information about its registered users. For instance, LinkedIn collects information that its users provide at the time of registration, including their name, email address, and/or mobile number. Users who register for LinkedIn's "premium" service, which offers enhanced functionality, must also provide payment information, which LinkedIn thereby collects and retains. In my training and experience, such registration information can evidence the actual identity of a LinkedIn user (e.g., by tying a credit card registered to a particular individual to a LinkedIn account engaged in criminal conduct).

174. LinkedIn also collects and retains information "profile" information provided by its registered users. This is information that appears on a LinkedIn user's profile page, which is accessible to other users of LinkedIn's network (subject to restrictions that a user may request with regard to other users who have the ability to access their profile page). The profile information collected and retained by LinkedIn includes information that users provide about their "education, work experience, skills, photo, city or area, and endorsements." The term "endorsements" typically refers to other LinkedIn users who purport to endorse a particular user's professional skills. In my training and experience, such profile information can serve as attribution evidence that links a particular individual to a LinkedIn account (e.g., where a person uses their phone to photograph themselves and then provides that same photograph to LinkedIn for use in their profile).

175. LinkedIn also collects and retains information that users post or upload to LinkedIn from their own devices, such as their resume (which they may submit to a third-party job posting on LinkedIn), their contacts (which they may submit to LinkedIn, in order to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

populate a list of contacts on LinkedIn). In my training and experience, such information can help to identify the actual user of LinkedIn's services (e.g., a user's resume can identify the user's actual identity).

176. LinkedIn also collects and retains data that other LinkedIn users post regarding a specific LinkedIn user, such as posts that refer to a LinkedIn user, contact lists and calendar entries that include that LinkedIn user, and third-party members (e.g., corporations) of LinkedIn's network whose services the LinkedIn user used. In my training and experience, information about the third parties who have relationships with NILSEN can help identify the other perpetrators of the scheme under investigation, by helping to identify the other LinkedIn users who posted about NILSEN, who listed NILSEN as a contact, or whose services NILSEN used. Indeed, as explained above, NILSEN appeared to tell KUNJU that he planned to use LinkedIn to recruit other Amazon employees who he could bribe.

177. LinkedIn also collects and retains information about a user's activity on the LinkedIn network, including the profile pages visited by a user, the searches run by a user, the IP address from which a user accessed LinkedIn, the device from which a user accessed LinkedIn, cookies generated at the time of access, and the user's location (where a user has consented to sharing such information). In my training and experience, such information can serve as evidence of various aspects of the scheme under investigation, including the actual identity of a LinkedIn account's user(s), the identity of other conspirators, and their state of mind (e.g., based on the types of searches they run while on LinkedIn's network). As explained above, NILSEN specifically expressed interest in mining LinkedIn's network to find other Amazon employees who he could bribe in exchange for taking favorable action for his clients. The efforts he took to identify those potential targets of his scheme serve as obvious evidence of his crimes.

178. LinkedIn also collects and retains information about messages exchanged between LinkedIn users, and other user activity with respect to messages they receive (e.g., whether they read the message, even though they did not respond to it). Here, given NILSEN's efforts to use LinkedIn in furtherance of the criminal scheme, and to recruit

additional potential co-conspirators through the LinkedIn network, there is probable cause that such messages will serve as evidence of the crimes under investigation.

BACKGROUND REGARDING DROPBOX

179. "Dropbox" refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage media such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an "offsite" storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual's computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at an offsite location, such as Dropbox's servers.

180. Dropbox provides a variety of online services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account numbers).

181. When the subscriber transfers a file into a Dropbox account, it is initiated at the user's computer, transferred via the internet to Dropbox's servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. For instance, in this case, by providing [redacted] access to Buddibox's Dropbox account at [redacted] email address ([redacted]@gmail.com), NUHANOVIC enabled [redacted] to view files that NUHANOVIC and others had uploaded to that account and, correspondingly, to upload files that NUHANOVIC and others could view in that account.

182. If the subscriber does not delete the content, the files can remain on Dropbox's servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

183. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

184. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

SEALING REQUEST

185. It is respectfully requested that the Court issue an order sealing all papers submitted in support of the requested warrant, including this affidavit, until the earliest of the following: (a) two weeks following the unsealing of any charging document in a matter for which the warrants were issued; (b) two weeks following the closure of the investigation for which the warrants were issued; or (c) sixteen months following issuance of the warrant, unless the Court, upon motion of the government for good cause, orders an extension of the sealing Order. I respectfully submit that sealing these documents is necessary because the information described within is relevant to an ongoing investigation. Premature disclosure of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

the contents of these documents may adversely affect the integrity of the investigation, including giving targets a chance to destroy evidence or take other steps to hinder the investigation.

CONCLUSION

186. Based on the forgoing, I believe there is probable cause to believe that evidence, instrumentalities, contraband, and/or fruits of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected Computer), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud), will be found in the SUBJECT ACCOUNTS, as more fully described in Attachments A-1 through A-7 to this Affidavit. I therefore request that the Court issue warrants authorizing a search of the SUBJECT ACCOUNTS, for the items more fully described in Attachments B-1 through B-7 hereto, incorporated herein by reference, and the seizure of any such items found therein.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

187. Based on the foregoing, I request that the Court issue the proposed search warrants. Because the warrants will be served on Google, Yahoo, Apple, Facebook, LinkedIn, Quora, and Dropbox, which will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

ANDREA L. DESANTO
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this 29 day of July, 2019.

HON. MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-1

Google Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the following accounts:

- amazonnate11[@]gmail.com ("SUBJECT ACCOUNT 1"),
- joe[@]digitalcheckmate.com ("SUBJECT ACCOUNT 2"),
- jn[@]sellerstrategies.com ("SUBJECT ACCOUNT 3"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 4"),
- kml[@]digitalcheckmate.com ("SUBJECT ACCOUNT 5"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 6"),
- freakdaze[@]gmail.com ("SUBJECT ACCOUNT 7"),
- [redacted]googlemail.com ("SUBJECT ACCOUNT 8"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 9"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 10"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 11"),
- [redacted][@]gmail.com ("SUBJECT ACCOUNT 12"),
- ellekaye11[@]gmail.com ("SUBJECT ACCOUNT 13"),
- rogerparkin69[@]gmail.com ("SUBJECT ACCOUNT 14"),
- [redacted][@]gmail.com ("SUBJECT ACCOUNT 15"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 16").

as well as all other subscriber and log records associated with SUBJECT ACCOUNTS 1 through 16, which are located at premises owned, maintained, controlled or operated by Google LLC ("Google"), an electronic communications service provider and remote that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California. Brackets have been placed in the names of SUBJECT ACCOUNTS 1 through 16 to ensure that they are not inadvertently hyperlinked and contacted.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-2

Yahoo Account to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the following account: [redacted]yahoo.com (hereinafter "**SUBJECT ACCOUNT 17**"), as well as all other subscriber and log records associated with SUBJECT ACCOUNT 17, which is located at premises owned, maintained, controlled or operated by Oath Holdings, Inc., formerly known as Yahoo Holdings, Inc. and doing business as Yahoo ("Yahoo"), an electronic communications service provider that accepts service of legal process at 701 First Avenue, Sunnyvale, California. Brackets have been placed in the name of SUBJECT ACCOUNT 17 to ensure that it is not inadvertently hyperlinked and contacted.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-3

Facebook Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the following accounts:

- The account bearing profile identification number 557853344 ("SUBJECT ACCOUNT 18"),
- The account bearing profile identification number 23004459 ("SUBJECT ACCOUNT 19"), and
- The account bearing profile identification number 607905026066065 ("SUBJECT ACCOUNT 20").

as well as all other subscriber and log records associated with SUBJECT ACCOUNTS 18 through 20, which are stored at premises controlled by Facebook, Inc., a electronic communications service provider headquartered in Menlo Park, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-4

Apple iCloud Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with (including all preserved data) the Apple iCloud accounts associated with the following Apple user identifiers:

- **kristenleccese[@]gmail.com**, bearing digital sign identifier 10075071322 ("SUBJECT ACCOUNT 21"), and
- **joe[@]digitalcheckmate.com**, bearing digital sign identifier 1712170805 ("SUBJECT ACCOUNT 22")

as well as all other subscriber and log records associated with SUBJECT ACCOUNTS 21 and 22, which are stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cuptertino, CA 95014. Brackets have been placed in the name of SUBJECT ACCOUNTS 21 and 22 to ensure that they are not inadvertently hyperlinked and contacted.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-5

LinkedIn Account to be Searched

The electronically stored data, information, communications, subscriber records, and log records contained in, related to, and associated with (including all preserved data), the LinkedIn account bearing screenname "joenilsenseo" ("SUBJECT ACCOUNT 23"), which is stored at premises controlled by LinkedIn Corporation, an electronic communications service headquartered in Sunnyvale, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-6

Quora Accounts to be Searched

The electronically stored data, information, communications, subscriber records, and log records contained in, related to, and associated with (including all preserved data), the Quora accounts registered under joe[@]digitalcheckmate.com ("SUBJECT ACCOUNT 24"), kristenleccese[@]gmail.com ("SUBJECT ACCOUNT 25"), and kml[@]digitalcheckmate.com ("SUBJECT ACCOUNT 26"), which are stored at premises controlled by Quora Inc., an electronic communications service headquartered in Mountain View, California. Brackets have been placed in the name of SUBJECT ACCOUNTS 24 through 26 to ensure that they is not inadvertently hyperlinked and contacted.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-7

Dropbox Account to be Searched

The electronically stored data, information, communications, subscriber records, and log records contained in, related to, and associated with (including all preserved data), the Dropbox account registered to [redacted]gmail.com, including number [redacted] ("SUBJECT ACCOUNT 27"), which is stored at premises controlled by Dropbox, Inc., an electronic communications service and remote computing service provider headquartered in San Francisco, California. Brackets have been placed in the name of SUBJECT ACCOUNT 27 to ensure that it is not inadvertently hyperlinked and contacted.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-1

I. Section I - Information to be disclosed by Google LLC, for search:

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Google LLC ("Google"), regardless of whether such information is located within or outside of the United States, including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

a. The contents of all emails associated with **SUBJECT ACCOUNTS 1 through 16 (from January 1, 2018 to the present)**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

d. any Google Chat/Messenger information and/or records, including any contact or friend list, time, date, and IP address logs for Chat and Messenger use, and any archived web messenger communications stored on servers;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. any Google Drive content (including backups of any apps stored on Google Drive) for the time period January 1, 2018 to the present;

f. any Google Search Console content for the time period January 1, 2018 to the present;

g. any Google Web & Activity content for the time period January 1, 2018 to the present;

h. any Google Chrome Sync content for the time period January 1, 2018 to the present;

i. any Google Location History content for the time period January 1, 2018 to the present;

j. any account history, including any records of communications between Google and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service.

This Search Warrant also requires Google to produce the following information for SUBJECT ACCOUNTS 1 through 16 (collectively the "Linked Subject Accounts"):

a. a list of all other accounts linked to SUBJECT ACCOUNTS 1 through 16 because of cookie overlap;

b. a list of all other accounts linked to SUBJECT ACCOUNTS 1 through 16 because of SMS phone number overlap;

c. a list of all other accounts linked to SUBJECT ACCOUNTS 1 through 16 because of recovery-email-address overlap; and

d. a list of all other accounts that shared the same creation IP address as SUBJECT ACCOUNTS 1 through 16 within 30 days of creation;

e. Subscriber records for each of the Linked Subject Accounts including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts.

f. All records and other information (**not including the contents of communications**) relating to the Linked Subject Accounts, including (for the time period January 1, 2018 to the present):

i. Records of user activity for each connection made to or from the Linked Subject Account(s), including log files; messaging logs; the date time, length, and method of connections, data transfer volume; user names; and source and destination Internet Protocol Addresses; cookie IDs; browser type;

ii. Information about each communication sent or received by the Linked Subject Account Account(s), including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);

iii. All records pertaining to devices associated with the Linked Subject Account to include serial numbers, model type/number, IMEI, phone numbers, MAC Addresses.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected Computer), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud), those

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

violations occurring from on or about January 1, 2018 through the present, for SUBJECT ACCOUNTS 1 through 16 listed on Attachment A-1, and any Linked Subject Accounts, including the following:

a. Content that serves to identify any person who uses or accesses SUBJECT ACCOUNTS 1 through 16, or who exercises in any way any dominion or control over the account;

b. Content that relates to planned, attempted, or successful conduct with respect to seller accounts operating on the Amazon Marketplace online platform, or products sold on that platform;

c. Content that relates to information maintained by Amazon in connection with the operation of the Amazon Marketplace, including information regarding the operation of the Amazon Marketplace, information regarding the participants in the Amazon Marketplace, information regarding products sold on the Amazon Marketplace, information regarding metrics of Amazon Marketplace activity, information relating to enforcement actions (e.g., suspensions and reinstatements) taken with respect to sellers on Amazon Marketplace, and information relating to communications between third parties and Amazon with respect to activity on the Amazon Marketplace;

d. Content that relates to persons (both fictitious and actual) and products involved in e-commerce;

e. Content relating to planned, attempted, or successful transfers of funds in connection with the crimes specified above;

f. Content relating to the recruitment of employees of Amazon (or Amazon-affiliated entities) to take actions in exchange for things of value, including commercial bribes;

g. Content that constitute communications in furtherance of the crimes set out above;

h. Content that evidences the state of mind of any person(s), including the user(s) of SUBJECT ACCOUNTS 1 through 16, with regard to the crimes set out above;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

i. Content that may identify assets including bank accounts, commodities accounts, trading accounts, personal property and/or real estate that may represent proceeds of fraud or are traceable to such proceeds;

j. Content that may reveal the current or past location of the individual or individuals using SUBJECT ACCOUNTS 1 through 16;

k. Content that may reveal the identities of and relationships between co-conspirators;

l. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over SUBJECT ACCOUNTS 1 through 16 as well as records or information that may reveal the true identities of these individuals;

m. Other log records, including IP address captures, associated with SUBJECT ACCOUNTS 1 through 16;

n. Subscriber records associated with SUBJECT ACCOUNTS 1 through 16, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

o. Records of communications between Google and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

p. Android identification number, MEID, and cellular telephone number

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

q. Information regarding accounts that are linked or associated with SUBJECT ACCOUNTS 1 through 16, or the Linked Subject Accounts.

The requested warrant authorizes a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-2

I. Section I - Information to be disclosed by Oath Holdings, Inc. ("Yahoo"), for search:

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Yahoo, regardless of whether such information is located within or outside of the United States, including any emails, records, files, logs, or information that has been deleted but is still available to Yahoo, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Yahoo is required to disclose the following information to the government for each account or identifier listed in Attachment A-2:

a. The contents of all emails associated with **SUBJECT ACCOUNT 17 (from January 1, 2018 to the present)**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All subscriber records associated with SUBJECT ACCOUNT 17, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Yahoo in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. all location data associated with the account from January 1, 2018 to the present, including but not limited to GPS, Wi-Fi, or cell tower proximity records related to the account and/or account contents;

e. Any web browsing or search history associated with the account from January 1, 2018 to the present; and

f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

This Search Warrant also requires Yahoo to produce the following information for SUBJECT ACCOUNT 17 (collectively the "Linked Subject Accounts"):

a. a list of all other accounts linked to SUBJECT ACCOUNT 17 because of cookie overlap;

b. a list of all other accounts linked to SUBJECT ACCOUNT 17 because of SMS phone number overlap;

c. a list of all other accounts linked to SUBJECT ACCOUNT 17 because of recovery-email-address overlap; and

d. a list of all other accounts that shared the same creation IP address as SUBJECT ACCOUNT 17 within 30 days of creation;

e. Subscriber records for each of the Linked Subject Accounts including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Yahoo in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. All records and other information (**not including the contents of communications**) relating to the Linked Subject Accounts, including (for the time period January 1, 2018 to the present):

i. Records of user activity for each connection made to or from the Linked Subject Account(s), including log files; messaging logs; the date time, length, and method of connections, data transfer volume; user names; and source and destination Internet Protocol Addresses; cookie IDs; browser type;

ii. Information about each communication sent or received by the Linked Subject Account Account(s), including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);

iii. All records pertaining to devices associated with the Linked Subject Account to include serial numbers, model type/number, IMEI, phone numbers, MAC Addresses.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected Computer), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud), those violations occurring from on or about January 1, 2018 through the present, for SUBJECT ACCOUNT 17 listed on Attachment A-2, and any Linked Subject Accounts, including the following:

a. Content that serves to identify any person who uses or accesses SUBJECT ACCOUNT 17, or who exercises in any way any dominion or control over the account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Content that relates to planned, attempted, or successful conduct with respect to seller accounts operating on the Amazon Marketplace online platform, or products sold on that platform;

c. Content that relates to information maintained by Amazon in connection with the operation of the Amazon Marketplace, including information regarding the operation of the Amazon Marketplace, information regarding the participants in the Amazon Marketplace, information regarding products sold on the Amazon Marketplace, information regarding metrics of Amazon Marketplace activity, information relating to enforcement actions (e.g., suspensions and reinstatements) taken with respect to sellers on Amazon Marketplace, and information relating to communications between third parties and Amazon with respect to activity on the Amazon Marketplace;

d. Content that relates to persons (both fictitious and actual) and products involved in e-commerce;

e. Content relating to planned, attempted, or successful transfers of funds in connection with the crimes specified above;

f. Content relating to the recruitment of employees of Amazon (or Amazon-affiliated entities) to take actions in exchange for things of value, including commercial bribes;

g. Content that constitute communications in furtherance of the crimes set out above;

h. Content that evidences the state of mind of any person(s), including the user(s) of SUBJECT ACCOUNT 17, with regard to the crimes set out above;

i. Content that may identify assets including bank accounts, commodities accounts, trading accounts, personal property and/or real estate that may represent proceeds of fraud or are traceable to such proceeds;

j. Content that may reveal the current or past location of the individual or individuals using SUBJECT ACCOUNT 17;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

k. Content that may reveal the identities of and relationships between co-conspirators;

l. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over SUBJECT ACCOUNT 17 as well as records or information that may reveal the true identities of these individuals;

m. Other log records, including IP address captures, associated with SUBJECT ACCOUNT 17;

n. Subscriber records associated with SUBJECT ACCOUNT 17, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Yahoo in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

o. Records of communications between Yahoo and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

p. Information identifying accounts that are linked or associated with SUBJECT ACCOUNT 17, or the Linked Subject Accounts.

The requested warrant authorizes a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrant in order to locate evidence, fruits, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-3

I. Information to be disclosed by Facebook for search:

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each account identified in Attachment A-3, **within fourteen (14) days of the issuance of this warrant**:

(a) All contact and personal identifying information for SUBJECT ACCOUNTS 18 through 20, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers

(b) All activity logs for SUBJECT ACCOUNTS 18 through 20, and all other documents showing the users' posts and other Facebook activities;

(c) All photos and videos uploaded by SUBJECT ACCOUNTS 18 through 20, including all photos and videos uploaded by any user that tag the user(s) of SUBJECT ACCOUNTS 18 through 20;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user(s) of SUBJECT ACCOUNTS 18 through 20 are members, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the users' access and use of Facebook applications;

(e) All other records of communications and messages made or received by the users of SUBJECT ACCOUNTS 18 through 20, including all private messages, chat history, video calling history, and pending "Friend" requests;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the accounts;

(h) All records of the accounts' usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the users have "liked";

(i) All information about the Facebook pages that the accounts are or were a "fan" of;

(j) All past and present lists of friends created by the accounts;

(k) All records of Facebook searches performed by the accounts;

(l) All information about the users' access and use of Facebook Marketplace;

(m) The types of service utilized by the users;

(n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(p) All records pertaining to communications between Facebook and any person regarding the users' Facebook accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected Computer), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud), those violations occurring from on or about January 1, 2018 through the present, for SUBJECT ACCOUNTS 18 through 20 listed on Attachment A-3 including the following:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Content that serves to identify any person who uses or accesses SUBJECT ACCOUNT 18 through 20, or who exercises in any way any dominion or control over the account;

b. Content that relates to planned, attempted, or successful conduct with respect to seller accounts operating on the Amazon Marketplace online platform, or products sold on that platform;

c. Content that relates to information maintained by Amazon in connection with the operation of the Amazon Marketplace, including information regarding the operation of the Amazon Marketplace, information regarding the participants in the Amazon Marketplace, information regarding products sold on the Amazon Marketplace, information regarding metrics of Amazon Marketplace activity, information relating to enforcement actions (e.g., suspensions and reinstatements) taken with respect to sellers on Amazon Marketplace, and information relating to communications between third parties and Amazon with respect to activity on the Amazon Marketplace;

d. Content that relates to persons (both fictitious and actual) and products involved in e-commerce;

e. Content relating to planned, attempted, or successful transfers of funds in connection with the crimes specified above;

f. Content relating to the recruitment of employees of Amazon (or Amazon-affiliated entities) to take actions in exchange for things of value, including commercial bribes;

g. Content that constitute communications in furtherance of the crimes set out above;

h. Content that evidences the state of mind of any person(s), including the user(s) of SUBJECT ACCOUNT 18 through 20, with regard to the crimes set out above;

i. Content that may identify assets including bank accounts, commodities accounts, trading accounts, personal property and/or real estate that may represent proceeds of fraud or are traceable to such proceeds;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

j. Content that may reveal the current or past location of the individual or individuals using SUBJECT ACCOUNT 18 through 20;

k. Content that may reveal the identities of and relationships between co-conspirators;

l. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over SUBJECT ACCOUNT 18 through 20 as well as records or information that may reveal the true identities of these individuals;

m. Other log records, including IP address captures, associated with SUBJECT ACCOUNT 18 through 20;

n. Subscriber records associated with SUBJECT ACCOUNT 18 through 20, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Facebook in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

o. Records of communications between Facebook and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

The requested warrant authorizes a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrant in order to locate evidence, fruits, and instrumentalities

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-4

I. Information to be disclosed by Apple for search

To the extent that the information described in Attachment A-4 is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for the SUBJECT ACCOUNTS listed in Attachment A-4, **within fourteen (14) days of the issuance of this warrant**:

a. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address(es) used to register the accounts, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the accounts (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the accounts, including stored or preserved copies of emails sent to and from the accounts (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the accounts (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, Bookmarks, Contacts, Safari Browsing History, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the accounts (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the accounts were accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

i. All records pertaining to communications between Apple and any person(s) regarding the accounts, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected Computer), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud), those violations occurring from on or about January 1, 2018 through the present, for SUBJECT ACCOUNTS 21 and 22 listed on Attachment A-4, including the following:

a. Content that serves to identify any person who uses or accesses SUBJECT ACCOUNT 21 and 22, or who exercises in any way any dominion or control over the accounts;

b. Content that relates to planned, attempted, or successful conduct with respect to seller accounts operating on the Amazon Marketplace online platform, or products sold on that platform;

c. Content that relates to information maintained by Amazon in connection with the operation of the Amazon Marketplace, including information regarding the operation of the Amazon Marketplace, information regarding the participants in the Amazon Marketplace, information regarding products sold on the Amazon Marketplace, information regarding metrics of Amazon Marketplace activity, information relating to enforcement actions (e.g., suspensions and reinstatements) taken with respect to sellers on Amazon Marketplace, and information relating to communications between third parties and Amazon with respect to activity on the Amazon Marketplace;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. Content that relates to persons (both fictitious and actual) and products involved in e-commerce;

e. Content relating to planned, attempted, or successful transfers of funds in connection with the crimes specified above;

f. Content relating to the recruitment of employees of Amazon (or Amazon-affiliated entities) to take actions in exchange for things of value, including commercial bribes;

g. Content that constitute communications in furtherance of the crimes set out above;

h. Content that evidences the state of mind of any person(s), including the user(s) of SUBJECT ACCOUNT 21 and 22, with regard to the crimes set out above;

i. Content that may identify assets including bank accounts, commodities accounts, trading accounts, personal property and/or real estate that may represent proceeds of fraud or are traceable to such proceeds;

j. Content that may reveal the current or past location of the individual or individuals using SUBJECT ACCOUNT 21 and 22;

k. Content that may reveal the identities of and relationships between co-conspirators;

l. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over SUBJECT ACCOUNT 21 and 22 as well as records or information that may reveal the true identities of these individuals;

m. Other log records, including IP address captures, associated with SUBJECT ACCOUNT 21 and 22;

n. Subscriber records associated with SUBJECT ACCOUNT 21 and 22, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Apple in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

o. Records of communications between Apple and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

The requested warrant authorizes a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-5

I. Information to be disclosed by LinkedIn for search:

To the extent that the information described in Attachment A-5 is within the possession, custody, or control of LinkedIn, including any messages, records, files, logs, or information that have been deleted but are still available to LinkedIn, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), LinkedIn is required to disclose the following information to the government for the SUBJECT ACCOUNT listed in Attachment A-5, **within fourteen (14) days of the issuance of this warrant**:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address(es) used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past devices and computers, and any devices used to access LinkedIn and LinkedIn-connected services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all profiles associated with the SUBJECT ACCOUNT listed in Attachment A-5, including descriptions of education, work experience, skills, profile photographs, endorsements, and profinder profiles;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. The contents and viewing history of all messages associated with the SUBJECT ACCOUNT listed in Attachment A-5, including stored or preserved copies of messages sent to and from the account (including all draft messages and deleted messages), the source and destination addresses associated with each message, the date and time at which each message was sent, the size and length of each message, the actual IP addresses of the sender and the recipient of the message (to the extent available), and information regarding the date and time (if any) at which the message was viewed by its recipient;

e. The contents of all data viewed, uploaded, or published by the SUBJECT ACCOUNT listed in Attachment A-5, including posts published on the LinkedIn platform, resume uploads, imported contact lists, and calendar data;

f. The contents of all data received by LinkedIn from others regarding the SUBJECT ACCOUNT listed in Attachment A-5, including content and news regarding the user(s) of the SUBJECT ACCOUNT, contact and calendar information about the user(s) of the SUBJECT ACCOUNT, and the SUBJECT ACCOUNT's user's usage of services provided by LinkedIn affiliates;

g. The contents of all data regarding the SUBJECT ACCOUNT's connection history, including the profile names of all connections, the profile names of all connection invitations, the SUBJECT ACCOUNT's history of accepting or rejecting connection invitations, the SUBJECT ACCOUNT's history of sending connection invitations, the SUBJECT ACCOUNT's history of following and unfollowing connections, and the SUBJECT ACCOUNT's history of removing connections;

h. The contents of all data regarding the SUBJECT ACCOUNT's use of the LinkedIn service, including activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), and data regarding the SUBJECT ACCOUNT's connections search history and job-application history;

i. All records and information regarding locations where the SUBJECT ACCOUNT was accessed;

j. All records pertaining to the types of service used;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

k. All records pertaining to communications between LinkedIn and any person(s) regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken; and

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected Computer), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud), those violations occurring from on or about January 1, 2018 through the present, for SUBJECT ACCOUNT 23 listed on Attachment A-5, including the following:

a. Content that serves to identify any person who uses or accesses SUBJECT ACCOUNT 23, or who exercises in any way any dominion or control over the account;

b. Content that relates to planned, attempted, or successful conduct with respect to seller accounts operating on the Amazon Marketplace online platform, or products sold on that platform;

c. Content that relates to information maintained by Amazon in connection with the operation of the Amazon Marketplace, including information regarding the operation of the Amazon Marketplace, information regarding the participants in the Amazon Marketplace, information regarding products sold on the Amazon Marketplace, information regarding metrics of Amazon Marketplace activity, information relating to enforcement actions (e.g., suspensions and reinstatements) taken with respect to sellers on Amazon Marketplace, and information relating to communications between third parties and Amazon with respect to activity on the Amazon Marketplace;

d. Content that relates to persons (both fictitious and actual) and products involved in e-commerce;

e. Content relating to planned, attempted, or successful transfers of funds in connection with the crimes specified above;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. Content relating to the recruitment of employees of Amazon (or Amazon-affiliated entities) to take actions in exchange for things of value, including commercial bribes;

g. Content that constitute communications in furtherance of the crimes set out above;

h. Content that evidences the state of mind of any person(s), including the user(s) of SUBJECT ACCOUNT 23, with regard to the crimes set out above;

i. Content that may identify assets including bank accounts, commodities accounts, trading accounts, personal property and/or real estate that may represent proceeds of fraud or are traceable to such proceeds;

j. Content that may reveal the current or past location of the individual or individuals using SUBJECT ACCOUNT 23;

k. Content that may reveal the identities of and relationships between co-conspirators;

l. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over SUBJECT ACCOUNT 23 as well as records or information that may reveal the true identities of these individuals;

m. Other log records, including IP address captures, associated with SUBJECT ACCOUNT 23;

n. Subscriber records associated with SUBJECT ACCOUNT 23, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by LinkedIn in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

o. Records of communications between LinkedIn and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

The requested warrant authorizes a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-6

I. Information to be disclosed by Quora for search:

To the extent that the information described in Attachment A-6 is within the possession, custody, or control of Quora, including any messages, records, files, logs, or information that have been deleted but are still available to Quora, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Quora is required to disclose the following information to the government for the SUBJECT ACCOUNTS listed in Attachment A-6, **within fourteen (14) days of the issuance of this warrant**:

a. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the dates on which the accounts were created, the length of service, the IP address(es) used to register the accounts, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past devices and computers, and any devices used to access Quora), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all account and profile information associated with the SUBJECT ACCOUNTS listed in Attachment A-6, including real name, contact information, photographs, the identity of users following and followed by the accounts, topics of interest, credentials, and other information provided by the accounts' users;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. The content of all information and content posted by the SUBJECT ACCOUNTS' users to the Quora platform (including editing history), including questions, answers, photos, and comments, as well as the metadata associated with all such content;

e. The content of all information regarding the SUBJECT ACCOUNTS' integrated service provider(s) and linked network(s), including whether the SUBJECT ACCOUNTS' users signed in or signed up to the Quora platform through a linked network, and the history of linking other network accounts to the Quora network. Such information shall also include information provided by linked network(s) regarding the SUBJECT ACCOUNTS' users, including login information, profile information, and payment information;

f. The content of all information automatically collected by Quora regarding the SUBJECT ACCOUNTS' activity on Quora, including search history, page views, dates and times of connections to the Quora platform, browser type, type of computer or mobile device, browser language, IP address, mobile carrier, unique device identifier, location information, and requested and referring URLs;

g. The content of all information regarding the SUBJECT ACCOUNTS' engagement with the Quora platform, including IP address and location, date and time stamp, user agent, Quora cookie IDs, as well as all information about user activity on third party sites and services that have embedded Quora pixels, widgets, plug-ins, buttons, or related services.

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Quora and any person(s) regarding the SUBJECT ACCOUNTS listed in Attachment A-6, including contacts with support services and records of actions taken; and

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Computer), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud), those violations occurring from on or about January 1, 2018 through the present, for SUBJECT ACCOUNTS 24 through 26 listed on Attachment A-6, including the following:

a. Content that serves to identify any person who uses or accesses SUBJECT ACCOUNTS 24 through 26, or who exercises in any way any dominion or control over the account;

b. Content that relates to planned, attempted, or successful conduct with respect to seller accounts operating on the Amazon Marketplace online platform, or products sold on that platform;

c. Content that relates to information maintained by Amazon in connection with the operation of the Amazon Marketplace, including information regarding the operation of the Amazon Marketplace, information regarding the participants in the Amazon Marketplace, information regarding products sold on the Amazon Marketplace, information regarding metrics of Amazon Marketplace activity, information relating to enforcement actions (e.g., suspensions and reinstatements) taken with respect to sellers on Amazon Marketplace, and information relating to communications between third parties and Amazon with respect to activity on the Amazon Marketplace;

d. Content that relates to persons (both fictitious and actual) and products involved in e-commerce;

e. Content relating to planned, attempted, or successful transfers of funds in connection with the crimes specified above;

f. Content relating to the recruitment of employees of Amazon (or Amazon-affiliated entities) to take actions in exchange for things of value, including commercial bribes;

g. Content that constitute communications in furtherance of the crimes set out above;

h. Content that evidences the state of mind of any person(s), including the user(s) of SUBJECT ACCOUNTS 24 through 26, with regard to the crimes set out above;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

i. Content that may identify assets including bank accounts, commodities accounts, trading accounts, personal property and/or real estate that may represent proceeds of fraud or are traceable to such proceeds;

j. Content that may reveal the current or past location of the individual or individuals using SUBJECT ACCOUNTS 24 through 26;

k. Content that may reveal the identities of and relationships between co-conspirators;

l. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over SUBJECT ACCOUNTS 24 through 26 as well as records or information that may reveal the true identities of these individuals;

m. Other log records, including IP address captures, associated with SUBJECT ACCOUNTS 24 through 26;

n. Subscriber records associated with SUBJECT ACCOUNTS 24 through 26, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Quora in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

o. Records of communications between Quora and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

The requested warrant authorizes a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-7

I. Section I - Items to be to be Provided by Dropbox for Search

To the extent that the information described in Attachment A-6 is within the possession, custody, or control of Dropbox, including any messages, records, files, logs, or information that have been deleted but are still available to Dropbox, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox is required to disclose the following information to the government for the SUBJECT ACCOUNT listed in Attachment A-7, **within fourteen (14) days of the issuance of this warrant**:

a. All electronically stored information and communications contained in SUBJECT ACCOUNT 27, including, any online storage account linked to SUBJECT ACCOUNT 27, all account registration information, user contact information, linked web addresses and posted images, content and logs;

b. All subscriber records associated with SUBJECT ACCOUNT 27, including name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, (including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

c. any and all other log records, including IP address captures, associated with SUBJECT ACCOUNT 27;

d. any address lists or buddy/contact lists associated with SUBJECT ACCOUNT 27; and

e. any records of communications between Dropbox, and any other person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected Computer), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud), those violations occurring from on or about January 1, 2018 through the present, for SUBJECT ACCOUNT 27 listed on Attachment A-7, including the following:

a. Content that serves to identify any person who uses or accesses SUBJECT ACCOUNT 27, or who exercises in any way any dominion or control over the account;

b. Content that relates to planned, attempted, or successful conduct with respect to seller accounts operating on the Amazon Marketplace online platform, or products sold on that platform;

c. Content that relates to information maintained by Amazon in connection with the operation of the Amazon Marketplace, including information regarding the operation of the Amazon Marketplace, information regarding the participants in the Amazon Marketplace, information regarding products sold on the Amazon Marketplace, information regarding metrics of Amazon Marketplace activity, information relating to enforcement actions (e.g., suspensions and reinstatements) taken with respect to sellers on Amazon Marketplace, and information relating to communications between third parties and Amazon with respect to activity on the Amazon Marketplace;

d. Content that relates to persons (both fictitious and actual) and products involved in e-commerce;

e. Content relating to planned, attempted, or successful transfers of funds in connection with the crimes specified above;

f. Content relating to the recruitment of employees of Amazon (or Amazon-affiliated entities) to take actions in exchange for things of value, including commercial bribes;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. Content that constitute communications in furtherance of the crimes set out above;

h. Content that evidences the state of mind of any person(s), including the user(s) of SUBJECT ACCOUNT 27, with regard to the crimes set out above;

i. Content that may identify assets including bank accounts, commodities accounts, trading accounts, personal property and/or real estate that may represent proceeds of fraud or are traceable to such proceeds;

j. Content that may reveal the current or past location of the individual or individuals using SUBJECT ACCOUNT 27;

k. Content that may reveal the identities of and relationships between co-conspirators;

l. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over SUBJECT ACCOUNT 27 as well as records or information that may reveal the true identities of these individuals;

m. Other log records, including IP address captures, associated with SUBJECT ACCOUNT 27;

n. Subscriber records associated with SUBJECT ACCOUNT 27, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Dropbox in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

o. Records of communications between Dropbox and any person purporting to be the account holder about issues relating to the account, such as technical

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

The requested warrant authorizes a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Sixteen (16) Google accounts, hosted at premises controlled by Google LLC, located at 1600 Amphitheatre Parkway, Mountain View, CA, more fully described in Attachment A-1

Case No. MJ19-350

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

Sixteen (16) Google accounts, hosted at premises controlled by Google LLC, located at 1600 Amphitheatre Parkway, Mountain View, CA, more fully described in Attachment A-1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B-1, for a list of information to be disclosed, incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before August 12, 2019 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any U.S. Magistrate Judge in West. Dist. of Washington .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: July 29, 2019 2:45 pm

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge
Printed name and title

USAO: 2018R01422

AO 93 (Rev. 11/13) Search and Seizure Warrant (2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-1

Google Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the following accounts:

- amazonnate11[@]gmail.com ("SUBJECT ACCOUNT 1"),
- joe[@]digitalcheckmate.com ("SUBJECT ACCOUNT 2"),
- jn[@]sellerstrategies.com ("SUBJECT ACCOUNT 3"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 4"),
- kml[@]digitalcheckmate.com ("SUBJECT ACCOUNT 5"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 6"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 7"),
- [redacted][@]googlemail.com ("SUBJECT ACCOUNT 8"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 9"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 10"),
- [redacted][@]gmail.com ("SUBJECT ACCOUNT 11"),
- [redacted][@]gmail.com ("SUBJECT ACCOUNT 12"),
- ellekaye11[@]gmail.com ("SUBJECT ACCOUNT 13"),
- rogerparkin69[@]gmail.com ("SUBJECT ACCOUNT 14"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 15"),
- [redacted]gmail.com ("SUBJECT ACCOUNT 16").

as well as all other subscriber and log records associated with SUBJECT ACCOUNTS 1 through 16, which are located at premises owned, maintained, controlled or operated by Google LLC ("Google"), an electronic communications service provider and remote that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California. Brackets have been placed in the names of SUBJECT ACCOUNTS 1 through 16 to ensure that they are not inadvertently hyperlinked and contacted.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-1

I. Section I - Information to be disclosed by Google LLC, for search:

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Google LLC ("Google"), regardless of whether such information is located within or outside of the United States, including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

a. The contents of all emails associated with **SUBJECT ACCOUNTS 1 through 16 (from January 1, 2018 to the present)**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

d. any Google Chat/Messenger information and/or records, including any contact or friend list, time, date, and IP address logs for Chat and Messenger use, and any archived web messenger communications stored on servers;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. any Google Drive content (including backups of any apps stored on Google Drive) for the time period January 1, 2018 to the present;

f. any Google Search Console content for the time period January 1, 2018 to the present;

g. any Google Web & Activity content for the time period January 1, 2018 to the present;

h. any Google Chrome Sync content for the time period January 1, 2018 to the present;

i. any Google Location History content for the time period January 1, 2018 to the present;

j. any account history, including any records of communications between Google and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service.

This Search Warrant also requires Google to produce the following information for SUBJECT ACCOUNTS 1 through 16 (collectively the "Linked Subject Accounts"):

a. a list of all other accounts linked to SUBJECT ACCOUNTS 1 through 16 because of cookie overlap;

b. a list of all other accounts linked to SUBJECT ACCOUNTS 1 through 16 because of SMS phone number overlap;

c. a list of all other accounts linked to SUBJECT ACCOUNTS 1 through 16 because of recovery-email-address overlap; and

d. a list of all other accounts that shared the same creation IP address as SUBJECT ACCOUNTS 1 through 16 within 30 days of creation;

e. Subscriber records for each of the Linked Subject Accounts including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts.

f. All records and other information (**not including the contents of communications**) relating to the Linked Subject Accounts, including (for the time period January 1, 2018 to the present):

i. Records of user activity for each connection made to or from the Linked Subject Account(s), including log files; messaging logs; the date time, length, and method of connections, data transfer volume; user names; and source and destination Internet Protocol Addresses; cookie IDs; browser type;

ii. Information about each communication sent or received by the Linked Subject Account Account(s), including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);

iii. All records pertaining to devices associated with the Linked Subject Account to include serial numbers, model type/number, IMEI, phone numbers, MAC Addresses.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1029 (Access Device Fraud), 1030 (Unauthorized Access to a Protected Computer), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud), those

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

violations occurring from on or about January 1, 2018 through the present, for SUBJECT ACCOUNTS 1 through 16 listed on Attachment A-1, and any Linked Subject Accounts, including the following:

a. Content that serves to identify any person who uses or accesses SUBJECT ACCOUNTS 1 through 16, or who exercises in any way any dominion or control over the account;

b. Content that relates to planned, attempted, or successful conduct with respect to seller accounts operating on the Amazon Marketplace online platform, or products sold on that platform;

c. Content that relates to information maintained by Amazon in connection with the operation of the Amazon Marketplace, including information regarding the operation of the Amazon Marketplace, information regarding the participants in the Amazon Marketplace, information regarding products sold on the Amazon Marketplace, information regarding metrics of Amazon Marketplace activity, information relating to enforcement actions (e.g., suspensions and reinstatements) taken with respect to sellers on Amazon Marketplace, and information relating to communications between third parties and Amazon with respect to activity on the Amazon Marketplace;

d. Content that relates to persons (both fictitious and actual) and products involved in e-commerce;

e. Content relating to planned, attempted, or successful transfers of funds in connection with the crimes specified above;

f. Content relating to the recruitment of employees of Amazon (or Amazon-affiliated entities) to take actions in exchange for things of value, including commercial bribes;

g. Content that constitute communications in furtherance of the crimes set out above;

h. Content that evidences the state of mind of any person(s), including the user(s) of SUBJECT ACCOUNTS 1 through 16, with regard to the crimes set out above;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

i. Content that may identify assets including bank accounts, commodities accounts, trading accounts, personal property and/or real estate that may represent proceeds of fraud or are traceable to such proceeds;

j. Content that may reveal the current or past location of the individual or individuals using SUBJECT ACCOUNTS 1 through 16;

k. Content that may reveal the identities of and relationships between co-conspirators;

l. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over SUBJECT ACCOUNTS 1 through 16 as well as records or information that may reveal the true identities of these individuals;

m. Other log records, including IP address captures, associated with SUBJECT ACCOUNTS 1 through 16;

n. Subscriber records associated with SUBJECT ACCOUNTS 1 through 16, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

o. Records of communications between Google and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

p. Android identification number, MEID, and cellular telephone number

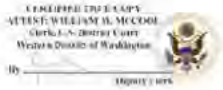
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

q. Information regarding accounts that are linked or associated with SUBJECT ACCOUNTS 1 through 16, or the Linked Subject Accounts.

The requested warrant authorizes a review of electronic storage media, electronically stored information, communications, and other records and information seized, copied or disclosed pursuant to the warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Magistrate Judge Michelle L. Peterson



UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

IN THE MATTER OF THE SEARCH OF: **SUBJECT ACCOUNTS 1 - 16**	NOS. MJ19-350 MOTION TO SEAL SEARCH WARRANTS AND RELATED MATERIALS **(FILED UNDER SEAL)**

The United States of America, by and through Brian T. Moran, United States Attorney for the Western District of Washington, and Siddharth Velamoor, Assistant United States Attorney, respectfully requests that these Search Warrants, Applications for Search Warrants, and related documents in this matter, including this Motion and its attendant Order, be sealed as set forth below, to protect the ongoing criminal investigation. The United States of America further respectfully requests that notwithstanding the requested sealing order, the Government retain the authority to produce the materials subject to this Court's sealing order as part of its discovery obligations in a criminal case.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Federal courts are empowered to seal documents in appropriate circumstances. *Cf.* Fed. R. Crim. P. 6(e)(4) (sealing of indictments). It is well-settled that federal courts have inherent authority to control papers filed with the court, *United States v. Shryock*, 342 F.3d 948, 983 (9th Cir. 2003), including the power to seal affidavits filed with search warrants in appropriate circumstances. In *Times Mirror Company v. United States*, 873 F.2d 1210 (9th Cir. 1989), the Court recognized that "information disclosed to the magistrate in support of the warrant request is entitled to the same confidentiality accorded other aspects of the criminal investigation." *Id.* at 1214. This inherent power may appropriately be exercised when disclosure of the affidavit would disclose facts that would interfere with an ongoing criminal investigation. *United States v. Napier*, 436 F.3d 1133, 1136 (9th Cir. 2006) (noting that a sealed search warrant protects the "government's interest in maintaining [the] integrity of ongoing criminal investigations and ensuring the safety of the informant").

In support of this request, the government states that the public disclosure of any of these materials at this juncture could jeopardize the government's ongoing investigation in this case because the case involves a suspected bribery and fraud scheme that targets Amazon and its customers, located in Western Washington, and elsewhere. Although an Indictment has been filed in connection with this investigation, not all of the subjects of the investigation are aware of the government's investigation into their conduct, including as described in the search warrant materials. Thus public disclosure of these materials could cause subjects of the investigation to destroy evidence or flee prosecution.[1]

//

//

[1] On or about July 29, 2019, at the time it issued the warrant in this matter, this Court previously ordered these materials sealed. That sealing Order has since expired. Through this Motion, the Government seeks to extend the sealing period.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Therefore, the United States of America respectfully requests that the documents in this case be sealed until the earliest of the following: (a) two weeks following the closure of the investigation for which the warrants were issued; or (b) December 31, 2021, unless the Court, upon motion of the government for good cause, orders an extension of the Order.

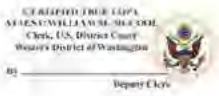
DATED this 7th day of December, 2020.

Respectfully submitted,
BRIAN T. MORAN
United States Attorney

/s/ Siddharth Velamoor
SIDDHARTH VELAMOOR
Assistant United States Attorney

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Magistrate Judge Michelle L. Peterson



UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

IN THE MATTER OF THE SEARCH OF: **SUBJECT ACCOUNTS 1 - 16**	**NO. MJ19-350** **ORDER SEALING SEARCH WARRANTS AND RELATED MATERIALS** **(FILED UNDER SEAL)**

Based upon the motion of the United States, and the representations made therein, and good cause having been show:

IT IS HEREBY ORDERED that the search warrants, search warrant returns, applications and affidavits in support of the same, and all attachments in this matter, along with this motion and order, shall be sealed and shall remain sealed until the earliest of the following: (a) two weeks following the closure of the investigation for which the warrants were issued; or (b) December 31, 2021, unless the Court, upon motion of the government for good cause, orders an extension of the Order. Nothing in this Order is intended to create or supersede any other applicable obligation under law.

IT IS FURTHER ORDERED, that on or before the earliest of the dates specified above, the government shall file a motion in which it either (1) provides good cause for a further order of this Court permitting these documents to remain under seal for an additional period of time, or (2) requests an order of this Court to unseal this warrant and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

all related documents, including the motion and order to seal the same. In the event the government fails to file the motion required by this Order on or before the earliest of the three triggering events, and the Court has not otherwise extended the sealing period following a showing of good cause by the government, the Clerk of Court shall unseal this warrant and all related documents without further order of the Court.

IT IS SO ORDERED.

DATED this 8th day of December, 2020.

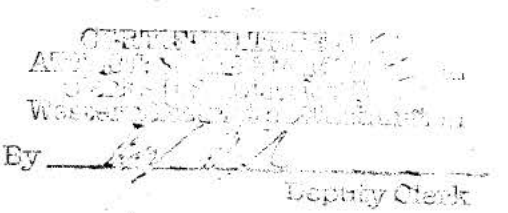
MICHELLE L. PETERSON
United States Magistrate Judge

Presented by:

/s/ Siddharth Velamoor
SIDDHARTH VELAMOOR
Assistant United States Attorney

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Magistrate Judge Mary Alice Theiler



UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MJ19-350

IN THE MATTER OF THE SEARCH OF: **SUBJECT ACCOUNTS 1 - 27**	**ORDER SEALING SEARCH WARRANTS AND RELATED MATERIALS** **(FILED UNDER SEAL)**

Based upon the motion of the United States, and the representations made therein, and good cause having been show:

IT IS HEREBY ORDERED that the search warrants, search warrant returns, applications and affidavits in support of the same, and all attachments in this matter, along with this motion and order, shall be sealed and shall remain sealed until the earliest of the following: (a) two weeks following the unsealing of any charging document in a matter for which the warrants were issued; (b) two weeks following the closure of the investigation for which the warrants were issued; or (c) sixteen months following issuance of the warrant, unless the Court, upon motion of the government for good cause, orders an extension of this Order. Nothing in this Order is intended to create or supersede any other applicable obligation under law.

IT IS FURTHER ORDERED, that on or before the earliest of the dates specified above, the government shall file a motion in which it either (1) provides good cause for a further order of this Court permitting these documents to remain under seal for an

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

additional period of time, or (2) requests an order of this Court to unseal this warrant and all related documents, including the motion and order to seal the same. In the event the government fails to file the motion required by this Order on or before the earliest of the three triggering events, and the Court has not otherwise extended the sealing period following a showing of good cause by the government, the Clerk of Court shall unseal this warrant and all related documents without further order of the Court.

IT IS SO ORDERED.

DATED this 29 day of July, 2019.

MARY ALICE THEILER
United States Magistrate Judge

Presented by:

/s/ Siddharth Velamoor
SIDDHARTH VELAMOOR
Assistant United States Attorney

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Magistrate Judge Mary Alice Theiler

CERTIFIED TRUE COPY
ATTEST
Clerk, U.S. District Court
Western District of Washington
By _____ Deputy Clerk

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

IN THE MATTER OF THE SEARCH OF: Sixteen (16) Google accounts, hosted at premises controlled by Google LLC, located at 1600 Amphitheatre Parkway, Mountain View, California 94043	CASE NO. MJ19-350 ORDER FOR NONDISCLOSURE **(FILED UNDER SEAL)**

The United States has submitted an application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding Google LLC ("Provider"), an electronic communication service provider and/or a remote computing service from which the Government has requested certain records and information pursuant to the above-captioned search warrant, not to notify any person (including the subscribers and customers of the account(s) listed in the subpoena) of the existence of the subpoena until further order of the Court.

The Court determines that there is reason to believe that notification of the existence of the search warrant will seriously jeopardize the investigation or unduly delay a trial, including by giving the targets of this investigation an opportunity to destroy or tamper with evidence, and change patterns of behavior. *See* 18 U.S.C. § 2705(b).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

IT IS THEREFORE ORDERED pursuant to 18 U.S.C. § 2705(b) that Provider shall not disclose the existence of the search warrant, or this Order of the Court, to the listed subscriber or to any other person, for a period of one year, unless and until otherwise authorized to do so by the Court, except that Provider may disclose the search warrant to an attorney for Provider for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

DATED this 29 day of July, 2019.

MARY ALICE THEILER
United States Magistrate Judge

Presented by:

/s/ *Siddharth Velamoor*
SIDDHARTH VELAMOOR
Assistant United States Attorney

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Sixteen (16) Google accounts, hosted at premises controlled by Google LLC, located at 1600 Amphitheatre Parkway, Mountain View, CA, more fully described in Attachment A-1

Case No. MJ19-350

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

Sixteen (16) Google accounts, hosted at premises controlled by Google LLC, located at 1600 Amphitheatre Parkway, Mountain View, CA, more fully described in Attachment A-1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B-1, for a list of information to be disclosed, incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before August 12, 2019 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any U.S. Magistrate Judge in West. Dist. of Washington .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: July 29, 2019 2:45 pm

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge
Printed name and title

USAO: 2018R01422

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
MJ19-350	7/30/2019 @ ~ 11:20am	NA

Inventory made in the presence of: SA Andrea L DeSanto

Inventory of the property taken and name of any person(s) seized:

(1) Blu-Ray Disc containing search warrant return material for the accounts listed in Attachment A

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 11/28/23

Executing officer's signature

Special Agent Donald Santiso

Printed name and title